Ministry of Education and Science of Ukraine

KHARKIV NATIONAL UNIVERSITY OF RADIO ELECTRONICS

ISMA UNIVERSITY

NATIONAL AVIATION UNIVERSITY

INSTITUTE FOR INFORMATION RECORDING

LVIV POLYTECHNIC NATIONAL UNIVERSITY

THE MILITARY ACADEMY OF THE ARMED FORCES OF AZERBAIDJAN REPUBLIC

Fourth International
Scientific and Technical Conference

«COMPUTER AND INFORMATION SYSTEMS AND TECHNOLOGIES»

April 22 – 23, 2020

Kharkiv 2020

Fourth International Scientific and Technical Conference «COMPUTER AND INFORMATION SYSTEMS AND TECHNOLOGIES». Kharkiv: NURE. 2020. – 90 p.

This publication is prepared by
Department of Electronic Computers
KHARKIV NATIONAL UNIVERSITY OF RADIO ELECTRONICS (NURE)

61166, Ukraine,
Kharkiv, 14 Nauki ave.
tel: +38 (057) 702-13-54
E-mail: info@csitic.com

ISBN 978-617-7645-96-1

PROGRAM COMMITTEE CO-CHAIRS

DODONOV Alexander	Dr.S., Prof., Institute for Information Recording of the National Academy of Sciences of Ukraine, *(Kyiv, Ukraine)*
FEDASYUK Dmitry	Dr.S., Prof., Lviv Polytechnic National University *(Lviv, Ukraine)*
KORCHENKO Alexander	Dr.S., Prof., National Aviation University *(Kyiv, Ukraine)*
MASHTALIR Volodymyr	Dr.S., Prof., Kharkiv National University of Radio Electronics *(Kharkiv, Ukraine)*
RUBAN Igor	Dr.S., Prof., Kharkiv National University of Radio Electronics *(Kharkiv, Ukraine)*
BAYRAMOV Agalar Azad ogly	Dr.S., Prof., The Military Academy of the Armed Forces of Azerbaidjan Republic *(Baku, Azerbaijan)*
DJAKONS Deniss	Dr.oec, Associate professor, Rector, ISMA University *(Riga, Latvia)*
KARPINSKI Mikolaj	Dr.S., prof. Chairman of Department of Computer Science and Automatics, University of Bielsko-Biala *(Bielsko-Biala, Poland)*
LEVASHENKO Vitaliy	Prof. Ing., PhD, University of Zilina *(Zilina, Slovakia)*

MEMBERS OF PROGRAM COMMITTEE

ALEXEYEV Mikhail	Dr.S., Prof., Dnipro Polytechnic National Technical University *(Dnipro, Ukraine)*
AKHMETOV Bakhytzhan Srazhatdinovich	Dr.S., Prof., Kazakh National Technical University named after K.I.Satpayev, Institute of Information and Telecommunication Technologies *(Almaty, Kazakhstan)*
BARABASH Oleg	Dr.S., Prof., State University of Telecommunications *(Kyiv, Ukraine)*
HASHIMOV Elshan Giyas	Dr.S., Prof., The Military Academy of the Armed Forces of Azerbaidjan Republic *(Baku, Azerbaijan)*
KOCHURKO Pavel	Ph.D., Assoc., Brest State Technical University *(Brest, Belarus)*
KOVALENKO Andriy	Dr.S., Prof., Kharkiv National University of Radio Electronics *(Kharkiv, Ukraine)*
KOSENKO Viktor	Dr.S., Prof., State Enterprise "Kharkiv Research Institute of Mechanical Engineering" *(Kharkiv, Ukraine)*
KUCHUK Heorhii	Dr.S., Prof. National Technical University "Kharkiv Polytechnic Institute" *(Kharkiv, Ukraine)*
LEVCHUK Victor	Ph.D., Assoc., Gomel State University named after Francis Skaryna *(Gomel, Belarus)*
LEVYKIN Victor	Dr.S., Prof., Kharkiv National University of Radio Electronics *(Kharkiv, Ukraine)*
LEMESHKO Oleksandr	Dr.S., Prof., Kharkiv National University of Radio Electronics *(Kharkiv, Ukraine)*
LUKOVA-CHUIKO Nataliia	Dr.S., Assoc., Taras Shevchenko National University of Kyiv *(Kyiv, Ukraine)*
MASHTALIR Sergii	Dr.S., Prof., Kharkiv National University of Radio Electronics *(Kharkiv, Ukraine)*
MIKHAL Oleg	Dr.S., Assoc., Kharkiv National University of Radio Electronics *(Kharkiv, Ukraine)*
PRIKHODKO Sergey	Dr.S., Prof., Ukrainian State University of Railway Transport *(Kharkiv, Ukraine)*
SEMENOV Serhii	Dr.S., Prof., National Technical University "Kharkiv Polytechnic Institute" *(Kharkiv, Ukraine)*
SMELYAKOV Kirill	Dr.S., Prof., Kharkiv National University of Radio Electronics *(Kharkiv, Ukraine)*
FEDOROVICH Oleg	Dr.S., Prof., National Aerospace University "Kharkiv Aviation Institute" *(Kharkiv, Ukraine)*
FILATOV Valentin	Dr.S., Prof., Kharkiv National University of Radio Electronics *(Kharkiv, Ukraine)*

KHARCHENKO Vyacheslav	Dr.S., Prof., National Aerospace University “Kharkiv Aviation Institute” *(Kharkiv, Ukraine)*
CHUMACHENKO Igor	Dr.S., Prof., O.M. Beketov National University of Urban Economy in Kharkiv *(Kharkiv, Ukraine)*
TSYMBAL Alexander	Dr.S., Prof., Kharkiv National University of Radio Electronics *(Kharkiv, Ukraine)*
SHMATKOV Sergey	Dr.S., Prof., V. N. Karazin Kharkiv National University *(Kharkiv, Ukraine)*
GOPEJENKO Viktors	Dr.sc.ing., Prof., Vice Rector for Research, ISMA University *(Riga, Latvia)*
ZAITSEVA Elena	Prof. Ing., PhD, University of Zilina *(Zilina, Slovakia)*

CHAIRMAN OF THE ORGANIZING COMMITTEE

MARTOVYTSKYI Vitalii	Ph.D., Kharkiv National University of Radio Electronics *(Kharkiv, Ukraine)*

MEMBERS OF ORGANIZING COMEETTEE

YEREMENKO Oleksandra	Dr.S., Assoc., Kharkiv National University of Radio Electronics *(Kharkiv, Ukraine)*
YEREMINA Natalia	Ph.D., Kharkiv National University of Radio Electronics *(Kharkiv, Ukraine)*
CHALA Oksana	Ph.D., Assoc., Kharkiv National University of Radio Electronics *(Kharkiv, Ukraine)*
LIASHENKO Oleksii	Ph.D., Assoc., Kharkiv National University of Radio Electronics *(Kharkiv, Ukraine)*
MOVSESIAN Iana	Ph.D., Kharkiv National University of Radio Electronics *(Kharkiv, Ukraine)*
ROSINSKY Dmitry	Kharkiv National University of Radio Electronics *(Kharkiv, Ukraine)*
TKACHOV Vitalii	Ph.D., Kharkiv National University of Radio Electronics *(Kharkiv, Ukraine)*
FEDIUSHYN Oleksandr	Ph.D., Assoc., Kharkiv National University of Radio Electronics *(Kharkiv, Ukraine)*

Kharkiv National University of Radio Electronics celebrates its 90th anniversary in 2020

The history of Kharkiv National University of Radio Electronics is doubtless unique. It began in 1930 with foundion of building institute that graduated about three thousand specialists.

In 1944 the educational institution was reorganized into the Kharkiv Mining and Industrial Institute, and in 1947 - into the Mining Institute. In the 1957/58 academic year, the training of energy engineers in automation began. In 1962, Kharkiv Institute of Mining Machinery Manufactoring, Automation and Computer Engineering was found on the basis of the KhMI, and in 1966 the last reorganization into Kharkiv University of Radio Electronics took place.

During its existence, KhIRE was awarded the Order of the Red Banner of Labor, given name of prominent scientist in the field of rocket and space technology, academician Mikhaila Kuzmicha Yangel, and created Academy of Sciences of Applied Radio Electronics.

According to the Presidential Decree in 1993, KhIRE was awarded the status of technical university as a result of national and international recognition of high level. By the decree of the President of Ukraine in 2001,it was awarded the status of national university, since then it is Kharkiv National University of Radio Electronics. KNURE was awarded the Silver Stella and the diploma of winner of International Academic Ranking "Golden Fortune" in the nomination "Quality of the Third Millennium Learning", the Stella "Sofia Kyivska" in the nomination "Technical and Technological Universities of Ukraine", which is an undeniable confirmation of the university's recognition at the national level.

The KNURE has established and gained international recognition for more than 30 scientific schools, including those, who led them, 25 academicians from national and international academies.

Today, KNURE is one of the three best universities in Kharkiv. In 2018, the university became one and only among technical HEIs, which ranked among top ten universities of Ukraine in the highest passing points in all specialties, it became the seventh university in the country by number of entrants to the state order and the first in Kharkiv.

The University's scientists are actively involved in work of Ukrainian IEEE Section, and the university itself co-organizers of six IEEE conferences. Through the collaboration with partners from IT industry, university has opened modern laboratories that provide students with the opportunity to learn with the help of modern equipment and acquire up-to-date knowledge of IT world. In 2019 the first science park in Ukraine was created, combining the scientific potential of the university and the capacity of the industry. During 90 years of history, KNURE has become the flagship of technical universities of Ukraine, and KNURE graduates are qualified specialists of national and international companies.

DEVELOPMENT AND OPERATION OF COMPUTER AND INTELLIGENT INFORMATION SYSTEMS

DOI: https://doi.org/10.30837/IVcsitic2020201132

The model retrieves software behavior information using a hierarchical model of nested auto-associating neural networks

Martovytskyi Vitalii[1]
Ruban Ihor[2]
Bukin Ihor[3]
Smyrnov Lev[3]

[1]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, vitalii.martovytskyi@nure.ua
[2]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, ihor.ruban@nure.ua
[3]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, lev.smyrnov@nure.ua

Abstract. *The existing algorithms for searching for malicious code are imperfect. For the most part, search programs determine the presence of malicious code based on already known samples. Thus, as a part of the study, a model for extracting information from data was developed, containing hierarchically related basic elements based on deep noise-canceling auto-encoders. In addition, the requirements for the model and the necessary operation parameters were determined.*

Keywords: *auto-encoder, SAE, auto-associating neural networks, malware.*

I. Introduction and Problem statement

The existing algorithms for searching for malicious code are imperfect. For the most part, search programs determine the presence of malicious code based on already known samples.

One of the drawbacks of this approach is the need to obtain a copy of the malware before extracting the pattern necessary for its future detection. Obtaining a copy of new or unknown malware usually entails infection or attack on a computer system.

To complicate matters, an increasing number of malware variants are automatically generated per day. A recent Symantec report [1] shows that the number of new malware at the beginning of February 2019 increased by 36 percent compared to last year, and the total number of samples exceeded 500 million.

Most modern virus attacks today are aimed at specific targets. Thus, the number of corporate infections in 2019 increased by 12% compared to 2018.

Modern technologies allow the use of artificial intelligence systems and data mining in almost any field of computer science, and, in particular, in information security.

The purpose of this report is to describe a mathematical model capable of extracting information about the behavior of software using a hierarchical model of nested auto-associating neural networks, which is resistant to non-informative transformations and is able to highlight the most important features of malicious software.

II. Problem solution and Results

In recent years, neural networks have proven successful in creating invariant representations for complex data [2], and the presented method attempts to use similar principles to generate invariant representations for malicious programs.

The basis of the proposed model is represented by neural networks grouped in layers $L_0, L_1, \ldots, Lc$ and connected sequentially with each other. Each layer is a fragment of a hierarchical chain, receiving as input data the data processing results, transformed to the lower level presentation layer, and sending the output data to the next level of the model.

Each layer is trained separately, implementing level-by-level model training. After training the first level of the model, the input data for the next layer is presented in the form of transformation results of the previous level that was trained earlier (output of the presentation layer of the previous model level). All levels are trained in the same way on the data transformed by the previous levels of the model, after which the process is repeated for the next levels.

The main component of the model is an auto-encoder neural network that functions separately within one hierarchy level of the model. An auto encoder consists of three main components — an encoder, a representation layer, and a decoder.

To train the auto-encoder, all parts of the auto-encoder are used, after which, the components of the encoder and representation layer are separated from the auto-encoder. Representation layers are later called upon to generate a compressed representation for the next level of the model.

The structural diagram of the model is shown in Fig. 1.

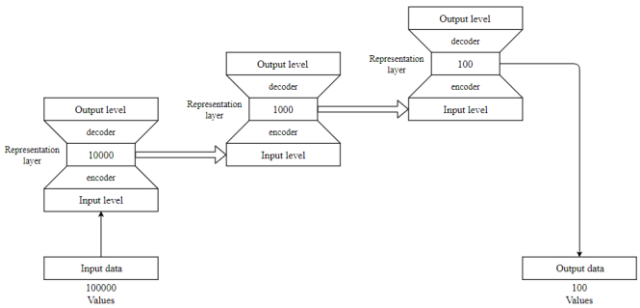


Figure 1. Structural diagram of the applied SAE architecture

Using the model to create a signature proceeds as follows. Let there be a desired recognition function g: $X \rightarrow Y$, the argument of which is a data set characterizing an aspect of the behavior of malware $x_n \in X$, presented as a vector of length n, and the values of functions are a set of values approximating

the aspect of behavior of malware $y_m \in Y$, varying depending on the task.

There is a subset of pairs of arguments and values of the function $D = \{\{x_0,y_0\},\ldots,\{x_m,y_m\}\}$. The presented model thus implements the function $h:X \rightarrow Y$, which would approximate the function g over its entire domain of definition, including the values outside of subset D[3].

To calculate the value of h (x), a data sample (vector) is fed to the input of the first layer of the trained model, and then a sequential transformation is performed while maintaining information content at each level of the model. Output activation at the last representation level of model is a vector with a lower dimension that defines a brief characteristic of the behavior of the sample based on a given aspect of the behavior.

At the same time, it is supposed to train models on various data sets characterizing various aspects of the behavior of the software instance. Thus, the aggregate characteristic of the behavior of an instance will consist of a composition of the results of all models.

Thus, the model is characterized by the following parameters:

– the number of representation levels $L_0,L_1,\ldots,L_c$;

– the required size of the last representation layer dim ($L_c^{n//2+1}$), where $dim(L)$ – the function for determining the dimension of the layer;

– the number of inner layers of each level of the model, consisting of coding L_i^e, representation L_i^r and decoding L_i^d layers, which are organized in the following order: $L_i^e{}_1$, ..., $L_i^e{}_m$, L_i^r, $L_i^d{}_1$, ..., $L_i^d{}_m$, and the total number of which will be equal $L_i n\_layers = 2m+1$;

– the function of reducing the dimension on each layer of the model $fR(Li)$, which returns the size of the representation layer required from the level;

– internal parameters of each level of the model:

- the number of neurons in each layer of each level;
- data normalization parameters;
- parameters for adding noise to the training data of the layer;
- parameters of layer activation functions;
- error function parameters;
- the number of epochs of learning level.

The number of representation levels is a parameter that is calculated dynamically, depending on the function of dimension reduction. The $fR(L_i)$ function takes the model level as an input, and calculates the size of the representation layer. It should be noted that for the first level of the model, the dimension of the first layer should be equal to the dimension of the input data, and for each subsequent layer, the dimension of the input layer will be equal to the result of calculating the function fR for the previous level:

$$\dim(L_0) = len(X), \quad (1)$$

Where $len(X)$ – the dimension of the input data,

$$\dim(L_i) = fR(L_{i-1}). \quad (2)$$

As part of the work, the following dimension reduction functions were implemented:

$$fR(L_i) = \frac{\dim(L_i^0)}{c}, \quad (3)$$

where c – certain constant, the function dim(L) – the function of determining the dimension of the layer, and L_i^0 – the input layer of the level.

Also, parameters calculated at runtime include the coefficient of dimension reduction on each layer of the model level (Per-Layer Reduction or PLR), which characterizes how many times the number of coding part neurons will decrease on each new layer and, accordingly, how many times will increase the number of neurons in the decoding layer:

$$\begin{cases} c*1000, & \dim(L_i^0) > c*1000 \\ \dim(L_i^0) - c*100, & \dim(L_i^0) > c*100 \\ \dim(L_i^0) - c*10, & \dim(L_i^0) > c*10 \end{cases} \quad (4)$$

n_layers – the number of layers at a given model level. With this, the number of neurons in each layer of each level is determined.

Learning curves for model levels are shown in Fig. 2.

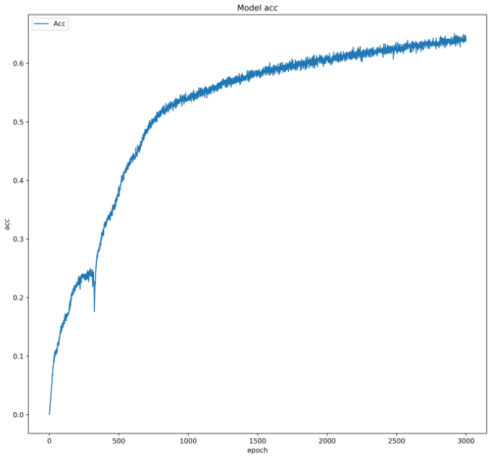


Figure 2. Learning curve of model levels

The model for processing the sample data consists of two layers of auto-encoders, which consistently reduce the dimensions 1006 > 250 > 50. Each level of this model was trained during 3000 training epochs, as a result, the average reconstruction accuracy is approximately 60%.

III. Conclusions

Thus, as a part of the study, a model for extracting information from data was developed, containing hierarchically related basic elements based on deep noise-canceling auto-encoders. In addition, the requirements for the model and the necessary operation parameters were determined.

IV. References

[1] 2019 Internet Security Threat Report, ISTR Volume 24 [Электронный ресурс] // Symantec – 2019, - access: https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-executive-summary-en.pdf – (data: 05.04.2020).

[2] Ruban, I., Martovytskyi, V., & Lukova-Chuiko, N. (2018). Approach to Classifying the State of a Network Based on Statistical Parameters for Detecting Anomalies in the Information Structure of a Computing System. *Cybernetics and Systems Analysis*, *54*(2), 302-309.

[3] Ruban, I. V., Martovytskyi, V. O., Kovalenko, A. A., & Lukova-Chuiko, N. V. (2019, September). Identification in Informative Systems on the Basis of Users' Behaviour. In 2019 IEEE 8th International Conference on Advanced Optoelectronics and Lasers (CAOL) pp. 574-577.

DOI: https://doi.org/10.30837/IVcsitic2020201135

Analyzing static calls in Java byte-code

Dvinskykh David[1]

Barkovska Olesia[2]

[1,2]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, david.dvinskykh@nure.ua

Abstract. *The major goal of research is to analyze and propose a new approach for static analysis of method calls in Java code and finding the class configurations using auxiliary libraries for reading and byte code search.*

Keywords: *byte-code, callgraph, challenges, java, jdk, jgrapht, jre, static analysis.*

I. Introduction and Problem statement

The software developer uses up to 90% of the time to read the code. For checking the places of creation and configuration in different classes, the developer manually checks each place using the usual file search, but due to human factor, there is a probability of missing some places [1]. To correct the situation, a tool is needed for automatic analyzing the code for the connection between its various parts. Many tools are free or paid, but with little functionality or many bugs [2].

The purpose of the study is to develop an approach for static analysis of method calls in Java and to find class configuration places.

Existing analogs (Java-callgraph, Javadepend) and the criteria against which they are compared are shown in Table 1.

Java-callgraph is a console application that requires the presence of Java Virtual Machine [3].

Javadepend is part of the proprietary JArchitect software product

Table 1. Table comparing existing software solutions

Criterias	java-callgraph	javadepend
Cost	Free	Paid
Open source	Open	Closed
License type	2-clause BSD license	N/A
Profiling	Exist	Non-exist
Output type	One	Many
CI/CD	Exist	Non-exist
Search with criteria	Non-exist	Exist

II. Problem solution and Results

The proposed analysis approach consists of three steps, shown in Fig. 1.

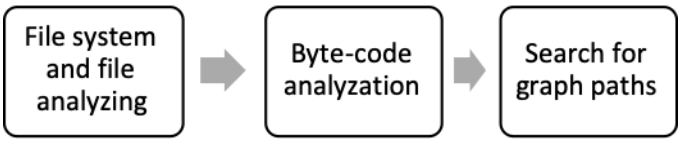


Figure 1. General approach to analyze calls

The first component should be used to collect files that have a class extension, then a list of all the files found is formed and passed to the input of the second component of the program, which will deal with the analysis and construction of vertices of the graph and the dependencies between them.

After constructing the entire graph, the third component begins its work, which looks all the way between the initial group of methods and the final group of methods. If filter criteria are specified, then in each path from start to finish, the program tries to find the first vertex that matches the filter.

Input parameters:

- paths to the files to be analyzed;
- names of packages start and end nodes of the graph;
- package names for the filter criterion;
- output format.

Each vertex that corresponds to the filter will be printed in the console or duplicated in a file. Each point has a name for the class, method, and archive where it was found. Javaagent is one of the JVM settings that allows you to specify an agent to run before launching the application. The agent executable is a standalone application that provides access to the byte code manipulation mechanism (java.lang.instrument) in the runtime.

Byte code can be parsed using the Apache BCEL library, and graphing is a third-party JGraphT library [4].

Criterion for finding paths in a graph - is the full or partial name of packages that contain classes with target methods.

The program should take the following paths:

- the path to the JAR file;
- the path to the WAR file;
- the path to the CLASS file;
- the path to a folder that contains any type of file, namely JAR, or WAR, or CLASS files.

III. Conclusions

Compared to other software solutions support for the filter criterion, additional output path, more output information for support for CI / CD processes were added.

IV. References

[1] Morenets S. Ideal code [Electronic resource] / Sergey Morenets // dou. - 2016. - Resource access mode: https://dou.ua/lenta/articles/perfect-code/.

[2] Martovytskyi, V. O., Kolodochkyn L. L."Stvorennia kros-platformnoi systemy zakhystu Web-servisiv i dodatkiv na osnovi XML-failiv dlia tekhnolohii ASP. NET." Systemy ozbroiennia i viiskova tekhnika 2 (2015): 122-123.

[3] Gousios G. java-callgraph: Java Call Graph Utilities [Online resource] / Georgios Gousios - Resource access mode: https://github.com/gousiosg/java-callgraph/blob/master/README.md.

[4] Explore Existing Architecture - Resource Access Mode:https://www.jarchitect.com/dependenciesview.

DOI: https://doi.org/10.30837/IVcsitic2020201136

Hybridization of the genetic algorithm with the apparatus of fuzzy sets

Skakalina Elena

National University "Yuri Kondratyuk Poltava Politechnics"
Pershotravnevyi ave. 24, Poltava, UA-36011, Ukraine
wboss@i.ua

Abstract. *Evolutionary algorithms are one of the effective methods for solving problems with high computational complexity, large dimension and search space. The use of evolutionary algorithms makes the question of choosing their settings and parameters relevant. The solution to this issue is difficult and significantly affects the quality of the resulting model. The paper considers the issue of determining the dimension of the current population during the operation of the genetic algorithm using the mathematical apparatus of fuzzy sets with a pentary membership scale. The proposed hybrid genetic algorithm has been tested on sets of test functions. A comparative analysis of the classical and hybrid genetic algorithms for the accuracy of solving the optimization problem of the general plan of logistics transportation is carried out.*

Keywords: *genetic algorithms, apparatus of fuzzy sets, optimization, logistics.*

I. Introduction and Problem statement

The vast majority of optimization tasks require a huge investment of time and computing resources. This is due to the need to sort out a huge number of different solutions. Moreover, by their computational complexity, such problems belong to the class of so-called NP-complete problems, that is, problems for which there is no deterministic polynomial algorithm. Therefore, to ensure that the best solution (global extremum) is found in such problems, it is necessary to perform exhaustive search, which in reality is not possible due to their large dimension [1-3]. Therefore, in practice, various metaheuristic algorithms are developed to solve such problems, which allow finding close to optimal (quasi-optimal) solutions. One of the approaches that can successfully solve the problem of increasing the efficiency and quality of solving complex optimization problems of large dimension is the integration of various scientific methods specific to such areas of computational intelligence as bio-inspired algorithms, fuzzy calculations, artificial neural networks [4-5]. Genetic algorithms (GA) as representatives of the metaheuristics group have become an important tool for solving optimization problems in various fields [6].

II. Problem solution and Results

Cost optimization is one of the most important tasks of transport logistics, the solution of which allows, under the existing restrictions on all types of resources used, to increase profits up to 25%. For logistics companies, this level of cost minimization can be achieved by constructing effective route plans for vehicles (V). A particularly significant effect of cost reduction can be achieved on large logistics networks. This circumstance forces researchers to search for efficient algorithms for solving the routing problem of vehicles that generate less costly routes and schedules. Heuristics (including GA) allow in some cases to generate solutions that increase the temporary solvency of the solution by almost two times.

At the initial stage (n = 0) of the classical genetic algorithm, an initial population of chromosomes is randomly generated, each of which is a sequence of genes encoding an alternative solution (for example, a chromosome may encode a variant of freight transport by a specific vehicle along a specific route). In this case, each gene may carry the values of the corresponding type of V and the length of the route. Then begins a cycle, at each iteration of which to the current population is consistently applied: the reproduction operator, randomly selects chromosomes for crossing, in proportion to their fitness function (determined by the values of the target function of the respective pairs - V & route); a crossover operator that mimics the generation of offspring chromosomes by borrowing separate sections of the parent's genetic code (the formation of new matching V pairs & route that inherited different V types and routes from different previously selected old pairs); a random mutation operator, with a given (small) probability, changes the chromosome in a random place at random; and, finally, the recombination operator that determines the chromosomes that will enter the next population (selects the most appropriate for the future evolution of a pair of V & route according to the value of their target function). The monetary value of the entire transport plan is used as the target function. The cycle continues until the maximum number of iterations n is reached or a satisfactory solution is obtained. The scheme of traditional GA:

BEGINNING */ * genetic algorithm * /*
Create an initial population;
Evaluate the suitability of each individual;
stop: = FALSE
UNTIL DOES NOT STOP EXECUTE
*BEGINNING / * create a new generation population * /*
REPEAT (population size / 2) TIMES
*BEGINNING / * playback cycle * /*
Choose two individuals with high adaptability from previous generation to cross;
Broken selected specimens and get two descendants;
Assess the suitability of descendants;
Place in a new generation of descendants;
END
IF the population agrees TO stop: = TRUE
END

In a hybrid GA (HGA), after creating the initial population and calculating the value of the fitness function for each pair of V & route, the apparatus of the theory of fuzzy sets (TFS) starts up [7]. We define a lot of linguistic variables "Value of fitness - function" as "Very Bad", "Bad", "Fair", "Good", "Very Good". Those pairs of V & route (chromosomes), the values of the fitness-functions of which fall into the FS "Very Bad", are

excluded from further processing. Thus, the dimension of the current population is reduced and the convergence time of the HGA is reduced, which is of relevance for problems of large dimension.

Hybrid GA Scheme:

BEGINNING */ * genetic algorithm * /*
Create an initial population;
Evaluate the suitability of each individual;
Formation of 5 fuzzy sets
"VB-very bad", "B-bad", "S-satisfactory", "G-good", "VG-very good"
*individuals depending on the suitability value / * FST * /*
Reducing the dimension of the initial population by removing from it the fuzzy set "VB"
stop: = FALSE
UNTIL NOT STOP EXECUTE
*BEGINNING / * create a new generation population * /*
REPEAT (population size / 2) TIMES
*BEGINNING / * playback cycle * /*
Choose two individuals with high adaptability from previous gen-eration to cross;
Broken selected specimens and get two descendants;
Assess the suitability of descendants;
Formation of 5 term sets "VD", "B", "S", "G", "VG" individuals depending on the value of the fitness function
*/ * FST * /*
Reducing the dimension of the initial population by removing from it the term set "VB"
END
IF the population agrees TO stop: = TRUE
END

The following HGA characteristics were used in the work: crossover type - single-point, parameter coding - real, which gives additional advantages in terms of HGA operation speed; the FS apparatus is used as a strategy for the formation of a new generation. The results of the first stage of experiments on test functions showed that the HGA showed the best results in terms of convergence rate and the probability of reaching an absolute optimum in comparison with classical GA (Table 1).

Table 1. Results of the first stage of testing

Type GA	Testing function		
	De Jong	Rosenbrock	Rastrigin
CGA	0.89	0.86	0.84
HGA	0.92	0.90	0.88

The results of the second experiment confirmed the results of the first. The value of the total cost of the entire transportation plan obtained using HGA showed more optimal results compared to CGA (Table 2).

Table 2. Value of the cost of the general transportation plan

Domain Object	CGA ($)	HGA ($)
DO#1	21598.70	16124.61
DO#2	83305.60	65984.84
DO#3	58179.20	47630.10
DO#4	112384.67	94781.93
DO#5	25384.98	12021.75
DO#6	97359.50	82840.36
DO#7	25292.50	16977.14
DO#8	11091.83	7308.28
DO#9	273595.78	223387.96
DO#10	308625.32	317943.95
DO#11	233056.21	215091.83

The proposed HGA is programmatically implemented on the .NET Framework and the MS Visual Studio development shell, the programming language is C #. Experiments were conducted to evaluate the capabilities of the author's HGA. The first stage of the HGA testing was carried out on the test functions of De Jong, Rozenbrock, Rastrigin [8-10]. The second stage of testing was carried out on real data obtained at the facilities of the following subject areas - the agricultural industry, the oil and gas industry, the logistics area in the process activity.

III. CONCLUSIONS

Evolutionary algorithms in general and genetic algorithms in particular have an advantage in solving optimization problems. This advantage is their ability to simultaneously operate with many solutions - the population, which allows us to reach a global extremum without getting stuck in local ones. Moreover, information about each individual in the population is encoded on the chromosome (genotype), obtaining the optimal solution (phenotype) is obtained after the implementation of the evolution process (selection, crossing, mutation) after decoding. The HGA proposed in the work allows the adaptive process of regulating the sizes of the initial and current populations using TFS. Dividing the current populations into five term sets makes it possible to implement parallel execution of HGAs (the so-called spatial methods for finding the extremum), which are generally more efficient than sequential (temporary) ones. In addition, in many subject areas of GA application in the formation of genes and chromosome structure, it is irrational to use binary coding and mutation, which is used in binary coding. This circumstance provides an additional advantage in increasing the temporary solvency of the HGA. Being randomly directed search methods on a variety of solutions, GAs are effectively used to solve NP-complete problems in decision support systems in complex organizational and technical systems.

REFERENCES

[1] Cohoon J.P., Karro J., Lienig J. Evolutionary algorithms for the physical design of VLSI circuit. In: Advances in Evolutionary Computing: Theory and Applications. A. Ghosh, S. Tsutsui (Eds.). Springer Verlag, London, 2003, pp. 683–712.

[2] Shervani N. Algorithms for VLSI physical design automation. Kluwer Acad. Publ., Dordrecht, 1995. 538 p.

[3] Alpert Ch.J., Dinesh P., Mehta D.P., Sapatnekar S.S. Handbook of algorithms for physical design automation. CRC Press, NY, USA, 2009.

[4] Ershov N.M. Non-uniform cellular genetic algorithms // Computer Research and Modeling, 2015, vol. 7, no. 3, pp. 775-780.

[5] Whitfield-Gabrieli S and Nieto-Castanon A, "Conn: a functional connectivity toolbox for correlated and anticorrelated brain networks," Brain Connect., vol. 2, no. 3, pp. 125–141, 2012. https://doi.org/10.1089/brain.2012.0073 PMID: 22642651.

[6] Kazakovtsev, L.A. An Approach to the Multi-facilityWeber Problem with Special Metrics /L.A.Kazakovtsev, P.S.Stanimirovic // European Modelling Symposium (EMS), 20-22 Nov. 2013.–Manchester:UkSim.–2013.–P. 119–124. DOI:10.1109/EMS.2013.21.

[7] Skakalina, E. (2018), «Development of Methodological Foundations of Logistical Intellectual Control of Complex Systems Based on Hybrid Heuristic Algorithms» / International Journal of Engineering & Technology.- 2018.- Vol. 7, No (4.8). – P.534-538. DOI: 10.14419/ijet.v7i4.8.27301

[8] De Jong K.A. Evolutionary computation a unified approach // A Bradford book. Cambridge: MA, USA. 256 p.

[9] Rosenbrock H.H., An automatic method for finding the greatest or least value of a function. - The Computer Journal 3, 1960. pp. 175–184.

[10] Rastrigin L. A., Systems of Extremal Control - Nauka, Moscow, 1974.

DOI: https://doi.org/10.30837/IVcsitic2020201139

Analysis of the current status of additional reality technologies

Kortyak Yelizaveta[1]
[1]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, yelyzaveta.kortiak@nure.ua

Bolohova Nataliia[2]
[2]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, nataliia.bolohova@nure.ua

Liashova Anastasiia[3]
[3]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine

Abstract. *The modern virtual reality industry holds a lot of potential since its investment activity has been increasing as well as the new breakthrough projects and technologies have been emerging. However, this field is still not so widespread. The article is devoted to the analysis of the VAMR-industry current state, to the research of the topical issues that do not allow the industry to become a part of the user's daily life, and to the search of their possible solutions. The definitions of 'VR', 'AR', 'MR' and the statistical data of the investment activity and the industry growth rate in 2016-2018 are given. The article considers the VAMR-industry problems from the perspective of a user in accordance with the price, usability, security and quality criteria. Here are described features of augmented reality technologies and their formats, basic principles and methods of its use. The specificity of the concept of augmented reality in the context of retail and industrial trade and its use in consumer and industrial marketing in the relevant markets. The tools and elements of augmented reality that influence the activity of enterprises, their positions and support in optimization of their digital strategy of the company are identified.*

***Keywords*:** *virtual reality industry; VAMR-industry; modern technologies; VAMR-industry problems; marketing instruments; reach of the target audience; customer behavior.*

I. REALITY TECHNOLOGIES

Currently, Virtual, Augmented and Mixed Reality (VR / AR / MR) is an emerging industry with great potential. The first steps towards the development of virtual reality technology were made in 1957, when the working prototype "Sensorama" (the Sensorama) was released.

However, the active growth of the VAMR industry began not too long ago. In 2012, a breakthrough was made in the industry - Oculus Rift virtual reality glasses were created. The appearance of this product marked a new stage in the development of VAMR.

Trends in the steady increase in growth and expansion of virtual technology in different areas not only characterize the current state of the market, but also create a number of complex and contradictory problems that require mandatory search and development of solutions.

II. PROS AND CONS OF REALITY TECHNOLOGIES

In practice, the difficulties in the development of the VAMR industry go far beyond terminology. The growth rate and investment attractiveness of the market are indicators that not only characterize the level of development of a given industry, but also reflect its scope and problems that need to be overcome.

- On the one hand:
  - VAMR is a promising industry (see Fig. 1). Transparency Market Research (TMR) estimates that VR and AR's global CAAGR (cumulative average annual growth rate) will reach US $ 547.20 billion by 2024 [1]. According to 2018 data, North America, which owns 80% of the world market, is the leader in the region's use of VR / AR technologies. [1] In 2017, the largest amount of investment in the VR / AR industry among all countries in the world belonged to the United States and amounted to $ 3.2 billion [2].

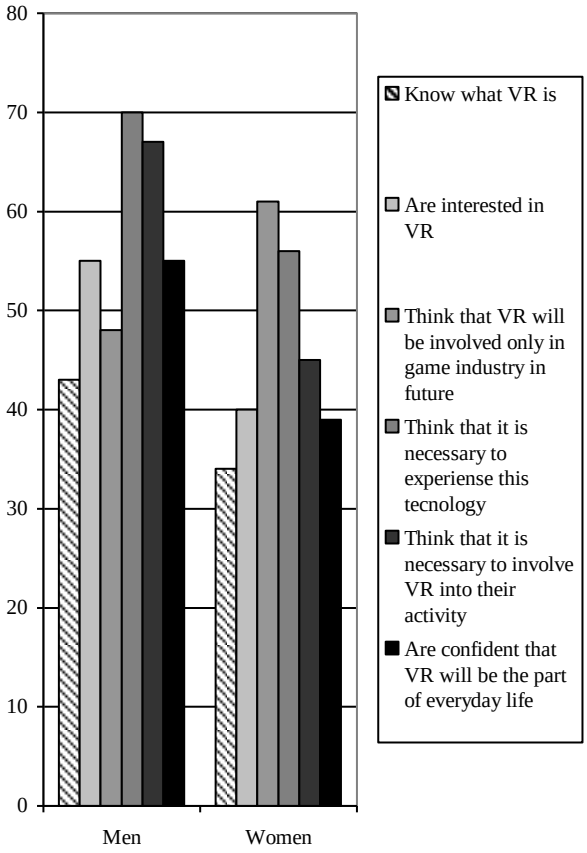


Figure 1. VR value in human life

  - VAMR solutions are used today in various fields: entertainment (games, cinema, sports broadcasts, theaters, museums, etc.), marketing, education,

medicine, industry, real estate, military-industrial complex, design, etc. there are many examples of successful cases using VAMR technologies worldwide and in many areas.

  - However, the gaming industry on a global scale still remains the area where VR devices are most in demand.
  - The annual VR market volume for gaming was $ 106 billion in 2016 [1].
- On the other hand:
  - Despite all the above trends and positive dynamics, the VAMR industry is still too young to become a full-fledged in the real-life of a user at the same level and scale as mobile communications, internet, or television. This thesis is confirmed in the downturn of 2017, when companies worldwide acquired only 24 thousand sets of AR points [2,3]. If you look at the dynamics of sales of VR points in the gaming market over the past two years, the following trends can be noted.
  - In 2016, Samsung Gear VR was the number one device sold (see Fig. 2). In 2017, this figure has dropped significantly. In most cases, the glasses were bundled with the Samsung Galaxy device of different versions, which, in our opinion, is the cause of the decline in sales.
  - Consumer motivation was related to buying a smartphone, not a VR helmet. At the same time, Playstation VR sales have more than doubled, driven by an increase in games on the platform [2].
- Conclusions:
  - The above data indicate that current and projected high rates of growth, investment activity, number of players in the market and production volumes characterize the VAMR industry as a whole, but do not explain the reasons for the lack of widespread availability, lack of mass virtual technology and mixed technologies in different segments (corporate and private clients).

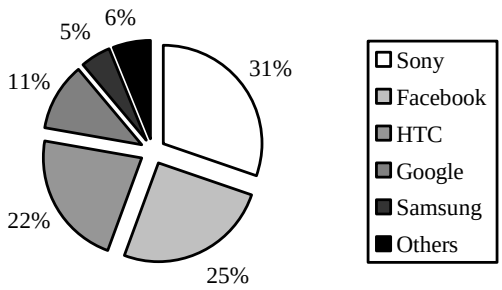


Figure 2. Usability of VR by companies

III. CONCLUSIONS

To sum up: expensive equipment and its maintenance, consumer dissatisfaction with the ergonomics of modern virtual machines designed and mixed reality, high risks of use and lack of solutions to ensure safe operation and the ability to improve the quality of output systems, lead to the fact that the VAMR industry is not yet mass and public.

In spite of the investment attractiveness and the considerable potential for growth, it is necessary to introduce such solutions that would overcome the above problems from the user's point of view and make a technological breakthrough to make VAMR technologies a part of everyday life.

Such a goal is achievable if a multidimensional consideration of the problems of the industry is not only from the point of view of the investor and the consumer, but also of the developer.

Here are several options to solve one of the problems:

– using augmented reality technology in a mobile-oriented university learning environment:
  - expand the capabilities of the laboratory facilities used to prepare students to work with real systems;
  - make available systems of high complexity and cost that were traditionally available only to specialists;
  - provides laboratory simulators with augmented reality interfaces that help to improve training;
  - motivates students to experiment and study.

REFERENCES

[1] Ivanova, A. (2018), “VR and AR technologies: advantages and barriers of usage”, Strategicheskie reshenija i risk-menedzhment, vol.3, pp.88-107.

[2] Bolohova, Nataliia, and Igor Ruban. "Image processing models and methods research and ways of improving marker recognition technologies in added reality systems." Innovative Technologies and Scientific Solutions for Industries 1 (7) (2019): 25-33.

[3] Williams, J. (2019), “Harvard Business Review”, [online], available at: https://bit.ly/2IlRiJy (Accessed 4 Oct. 2019).

[4] WEMOMACHINES (2019), “How WEMO use AR in manufacturing”, [online], available at: https://www.wemomachines.com/ (Accessed 2 Oct. 2019).

[5] Caudell T. P. Augmented reality: An application of heads-up display technology to manual manufacturing processes / T. P. Caudell, D. W. Mizell // Proceedings of the Twenty-Fifth Hawaii International Conference on System Sciences. January 7-10, 1992. Kauai, Hawaii. Volume 2: Software Technology Track / Edited by Jay F. Nunamaker, Jr. and Ralph H. Sprague, Jr. – Los Alamtos : IEEE Computer Society Press, 1992. – P. 659-669.

[6] Cieutat J.-M. Active Learning based on the use of Augmented Reality Outline of Possible Applications: Serious Games, Scientific Experiments, Confronting Studies with Creation, Training for Carrying out Technical Skills [Electronic resource] / Jean-Marc Cieutat, Olivier Hugues, Nehla Ghouaiel // International Journal of Computer Applications. – 2012. – Vol. 46. – No 20, May. – P. 31-36. – Access mode : https://hal.archives-ouvertes.fr/hal-00739730/document.

DOI: https://doi.org/10.30837/IVcsitic2020201140

Using the Adaptive Approach in the System of Monitoring the State of Grain Storage Technological Process

Liashenko Oleksii[1]
Znaiduk Vasyl[2]
Kazmina Daryna[3]

[1]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, e-mail: oleksii.liashenko@nure.ua*
[2]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, e-mail: karlsonman@gmail.com*
[3]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, e-mail: daryna.kazmina@nure.ua*

Abstract. *One of the requirements for modern monitoring systems is the timely detection of changes in the state of the system and ensuring continuous operation. Using the adaptive approach in the operation of the SCADA system, it is possible to ensure complying with the technological process parameters and obtaining quality products.*

Keywords: *controller, SCADA system, operating algorithm, microclimate, object, adaptive system.*

I. Introduction and Problem Statement

The SCADA systems are used to monitor and control technological processes in the agricultural industry. Modern requirements for the SCADA systems must have many parameters that will ensure trouble-free operation. Conventional engineering approaches and tools, such as development methodologies, architectural styles, modeling techniques, have limited capabilities to work with many quality attributes at the same time, and require important initial knowledge of the exact goals of the system and of every interaction that it enters and with which it can face in the future, should be known at the time of design. A possible solution to the problem is to build adaptive systems that can effectively adapt to failures, component replacement, and environmental changes with less human intervention or centralized operation [1-2]. If the system is adaptive, it implicitly means that it is flexible to adapt to dynamic changes in the environment, has a scalable ability to control the increase in size, and is able to cope with the evolution of its complexity.

II. Problem solution and Results

After analyzing the technological process of grain storage and drying, it can be determined that to maintain the microclimate in the granary for high-quality and long-term grain storage, as well as to be able to dry and cool the grain, a programmable logic controller with sensors of moisture and temperature of grain and air in the granary is used. The control system also includes a flowmeter to control the air supplied to the grain embankment and general air exchange in the granary.

In the presented study it is offered a mathematical model of temperature forecasting and correction, which describes the change of temperature and other microclimate parameters depending on the external environmental conditions, the algorithm of microclimate control is developed. When interrogating the sensors, the microcontroller determines the values of the microclimate parameters and then, in accordance with the agrotechnological requirements, issues control effects on the electrical equipment.

When designing the SCADA system, the following requirements were made: optimization of the electricity consumption of the object; possibility to connect electronic analytical scales with a unified output current signal of 4-20 mA; implementation of protective algorithms for the technological equipment; protection against incorrect sequence of switching on of the equipment; automatic stop of the equipment in case of emergencies; automation of working algorithms (choice of transport routes, start/stop/breaks); execution of protective algorithms; reduction of freelance and emergency situations; visualization of implementation of new technological processes on mnemonic circuits and reports; realization of object performance control, quantity of production at each stage); multi-level access system [3, 4].

The microclimate control subsystem includes:

1) maintaining the optimum air temperature during grain cooling to increase storage life;

2) sustaining humidity of air within 65-75% that provides the optimum one at storage of grain moisture equal to 14-16%.

3 controlling over the minimum required air flow depending on grain moisture

The developed SCADA provides support for the operation system that uses the adaptive approach to ensure quality while dynamically changing process parameters and system components.

III. Conclusions

The offered approach allows predicting the mutual influence of microclimate parameters and applying the adaptive working principle of electrical equipment with flexible hierarchical structure in real time while changing technological tasks to support them. An efficient automated system for monitoring temperature and humidity in the granary has been developed, which allows saving energy resources through using controllers with the adaptive control approach.

References

[1] Gang Feng, Rogelio Lozano, “Adaptive Control Systems”, Newnes, 1999, P. - 352

[2] I.D. Landau, R. Lozano,M. M'Saad, A. Karimi, Adaptive Control. Algorithms, Analysis and Applications. Springer, London, 2011. P. - 590.

[3] A. Kovalenko, H. Kuchuk, O. Lyashenko, “Distribution of resources of the largest phase system of processing big data for a high-intensive input power” Control, Navigation and Communication systems, Information Technology, Vol.5, №55, 2019, pp. 115-119

[4] Ruban, I., V. Martovytskyi, and N. Lukova-Chuiko. "Approach to Classifying the State of a Network Based on Statistical Parameters for Detecting Anomalies in the Information Structure of a Computing System." Cybernetics and Systems Analysis 54.2 (2018): 302-309.

DOI: https://doi.org/10.30837/IVcsitic2020201142

Problems of the detection systems usage and preventing intrusion into container environments

Misnik Oleksii

Pukhov Institute for Modelling in Energy Engineering, 15 General Naumov Str., Kyiv UA-03164, Ukraine, alexmisnik91@gmail.com

Abstract. *All the means of safety of the container environments are analyzed. There are generalized practical problems of using intrusion detection and prevention software, isolated application launch. Among them is emphasised functionality of this software. Emphasis is placed on the difficulties of implementing the privileged function. These difficulties lead to a decrease in the efficiency of its usage and, as a consequence, to the safety of container environments.*

Keywords: *container, container security, intrusion prevention system, intrusion detection system, docker.*

I. Introduction and Problem statement

Every year there is a growth of the information technology market. This determines the ways of developing container environments. While one of the important aspects of their usage is security. In particular, with the help of intrusion detection and prevention software, for example [1-2]: Snort, Suricata, Bro, Ossec, Prelude. The practical application of this software is limited by the difficulty of adapting their settings to ensure the safety of container environments. The following restriction also applies to isolated launch of applications, such as [3]: Seccomp, Apparmor, Selinux.

On the one hand, it is important to ensure the security of container environments by using intrusion detection and prevention software; isolated application launch. On the other hand, in practice it is easier said than done.

II. Problem solution and Results

The security of container environments through the usage of intrusion detection and prevention software involves the following issues:

- the similarity of models of information collection systems with each other and their disadvantages;
- the presence of a large number of false positive results in the detection of intrusions;
- software architecture limitations to detect and prevent intrusion while using in container environments [4];
- lack of effective means of automated analysis and visualization of information about incidents of information security;
- low efficiency and limited usage of software to detect and prevent intrusion in a container environment [5];
- the complexity of automated isolation of intrusion features by detection software [6].

Among them, one of the most significant problems is the limited software architecture for detecting and preventing intrusion in container environments [7]. As a consequence, their efficiency and safety in the container environment is reduced.

III. Conclusions

Therefore, the usage of intrusion detection and prevention software, isolated application launches for security in container environments is complicated to do in practice because of different architectural features. First of all, this is due to their limited functionality, in particular, when using the privileged function. Restrictions lead to a decrease in the efficiency of the specified software and, as a consequence, the difficulty of ensuring the security of container environments.

References

[1] T.I. Zorina, "Detection and prevention of attacks in computer networks" VISNIK OF THE VOLODYMYR DAHL EAST UKRAINIAN NATIONAL UNIVERSITY, Volodymyr Dahl East Ukrainian National University, No. 83, 2013, pp. 48-52

[2] Tereykovsky I., Korchenko A., Parashchuk T., Pedchenko Y., "Open intrusion detection systems analysis", Ukrainian Scientific Journal of Information Security,vol. 24, No. 3, 2018, pp. 201-216

[3] M.A. Kachanov, D.N. Kolegov, "Security analysis of the information flows by memory in the computer systems with functional and parametric associated entities", Mathematical Foundations of Computer Security, Tomsk State University, No. 2, 2008, pp. 76-80.

[4] A.S. Vishnyakov, A.E. Makarov, “Implementation of an external threat detection system in cloud computing”, Scientific journal, 2019

[5] Bondyakov Aleksey Sergeevich, "The basic modes of the intrusion prevention system (ids/ips suricata) for the computing cluster", International Scientific Journal "Modern Information Technology and IT-education", vol. 13, No. 3, 2017, p. 31-37

[6] O.I. Misnik, M.V. Antonishin, and V.V. Turcan, “Quality analysis web application vulnerability scanners”, Modeling and Information Technologies, No. 83, 2018, pp. 77-86.

[7] OWASP Docker-Security. [Online]. Available: https://github.com/OWASP/Docker-Security

DOI: https://doi.org/10.30837/IVcsitic2020201144

Distribution of Indivisible Resources During Big Data Processing

Heorhii Kuchuk[1]
Andriy Kovalenko[2]

[1]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, heorhii.kuchuk@nure.ua*
[2]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, andriy.kovalenko@nure.ua*

Abstract. *The method of load balancing for indivisible network resources when parallelizing Big Data processing is considered. A method for finding the optimal partitioning of a processing service into parallel processes is proposed.*

Keywords: *Big Data; indivisible resource; computing resource.*

I. Introduction and Problem Statement

One of the approaches used in Big Data processing is parallelization of computations [1-3]. In this case, one of the central issues in assessing the effectiveness of such processing is the analysis of processing requests to indivisible resources (IR), i.e. to those network elements that are available at any given time for no more than one request [4]. Queues to IR increase query execution time, which leads to a drop in QoS indexes. Obviously, uniform loading of IR will be the best option for increasing the speed of processing requests. Therefore, the purpose is to find such a partition of the Big Data processing process, in which the load balancing of indivisible resources is observed.

II. Problem Solution and Results

Let Big Data processing service (BDPS) F uses n of IR $f_1,\dots f_n$, each of which, with one call, provides the volume of a computing resource (CR) in the amount of $r_1,\dots r_n$ units, respectively. Suppose ones can decompose F BDPS into m ($m > n$) parallel processes (PP):

$$F = \bigcup_{i=1}^{m} \left(F_i \;\middle|\; F_{i_1} \cap F_{i_2} = \varnothing \;\; \forall i_1, i_2 \in \overline{1,m} \right), \qquad (1)$$

$$\forall j \in \overline{1,n} \left(\exists! F_i \;\middle|\; F_i \supset f_j, i = \max_{i'} \vartheta(i', j) \right), \qquad (2)$$

i.e., each PP includes no more than one IR, $\theta(i', j)$ is a frequency of f_j IR use by i' PP.

On the Cartesian product of $F \times F$ we introduce the following relation:

$$\varphi : \left(F_i, F_j \right) \to \lambda_{ij}, \qquad (3)$$

where λ_{ij} $(i \neq j)$ is the frequency of the direct transition from F_i PP to F_j PP to use the IR located on F_j, and λ_{ii} is the frequency of requests for its own IR of F_i PP (if the corresponding resource is not requested, then $\lambda_{ij} = 0$).

In such notation, the distribution of PP means finding such $\Re$ partition of F set into m disjoint (possibly empty) PPs in accordance with (1), in which the maximum load of IR is minimized:

$$\max_i \sum_{j=1}^{m} \lambda_{ij} \to \min, \quad F_i, F_j \in \Re. \qquad (4)$$

Objective function (4), in contrast to the standard ones used in such situations, is focused on uniform distribution the load among all IRs. In this case, it is necessary to meet the requirements for R_c computing resource allocated for F BDPS, i.e.

$$\sum_{i=1}^{m} r_i \sum_{j=1}^{m} \lambda_{ij} \le R_c. \qquad (5)$$

The formulated problem (1) - (3) for large values of m and n results in a large volume of calculations and, when applying various exact enumeration algorithms, does not provide a solution in an acceptable time. To solve it, we represent F set in the form of vertices of a fully connected graph of $G = \langle F, F \times F, \Xi, \varphi \rangle$, where the arcs of the graph are given by $F \times F$ Cartesian product; $\Xi = \{ r_i \}$ is a set of vertex weights; relation φ is a set of weights of the arcs of a graph. Then the set of solutions to problem (1) - (3) is the set of all possible cuts of G graph into m subgraphs. The problem can be reduced to partitioning into m maximally internally stable subgraphs with a minimum of adjacent vertices. To determine the maximally internally stable vertices of the graph, one can use the Bron and Carbosh algorithm, which is characterized by a small computational complexity that does not rapidly increase with increasing graph dimension.

III. Conclusions

Thus, load balancing for indivisible network resources allows to speed up Big Data processing. The optimal structure of parallel processing can be constructed by finding the corresponding cuts of a fully connected graph.

References

[1] Kuchuk G., Kovalenko A., Komari I.E., Svyrydov A., Kharchenko V. Improving big data centers energy efficiency: Traffic based model and method. *Studies in Systems, Decision and Control*, vol 171. Kharchenko, V., Kondratenko, Y., Kacprzyk, J. (Eds.). Springer Nature Switzerland AG, 2019. Pp. 161-183. DOI: http://doi.org/10.1007/978-3-030-00253-4_8

[2] Kharchenko V, Andrashov A, Sklyar V, Kovalenko A, Siora O. Gap-and-imeca-based assessment of i&C systems cyber security. *Complex Systems and Dependability*. Springer, Berlin, Heidelberg, 2013, pp. 149-164.

[3] Ruban, I., Kuchuk, H. and Kovalenko A. (2017), "Redistribution of base stations load in mobile communication networks", *Innovative technologies and scientific solutions for industries*, No 1 (1), P. 75–81, doi : https://doi.org/10.30837/2522-9818.2017.1.075.

[4] Kuchuk G., Nechausov S., Kharchenko, V. Two-stage optimization of resource allocation for hybrid cloud data store. *International Conference on Information and Digital Technologies. Zilina*, 2015. P. 266-271. DOI: http://dx.doi.org/10.1109/DT.2015.7222982

RELIABILITY AND SAFETY ASSURANCE TECHNOLOGIES FOR COMPUTER AND INFORMATIONAL SYSTEMS

DOI: https://doi.org/10.30837/IVcsitic2020201355

Hardware Obfuscation Using High Level Aggregation

Gorbachov Valeriy[1]
Abdulrahman Kataeba Batiaa[1]
Ponomarenko Olha[1]
Kotkova Oksana[1]

[1]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, valeriy.gorbachov@nure.ua*

Abstract. *The main principle of the proposed techniques is design obfuscation method to achieve hardware security. In the work we consider the reconfigurable-based obfuscation in the post-fabrication stage of IC. We address the need to add reconfigurable-logic stage to the development cycle. This technique may be considered as a preventative measure concealing some of the design from an attacker. In other words, it hides the exact functionality and schematic of an IC until after the reconfigurable logic has been programmed.*

Keywords: *security; reference monitor; hardware design obfuscation; hardware Trojan detection; hardware Trojan prevention; countermeasures.*

I. INTRODUCTION

With increasing computing power and integration density, several issues in design, performance and manufacturing of ICs have emerged. Moreover, increasing power consumption, increased cost of testing and verification, and complexities in manufacturing devices are the some of the major issues with IC design and manufacturing. To make such design and manufacturing feasible, an IC design house is commonly aided by the following external tools: the sophisticated software tools (EDA), that facilitates design, verification and testing of modern ICs; preverified, high performance, functional hardware IPs design facilities, which help to reduce the design time, improve reliability; the fabrication facilities where the design is actually manufactured and sometimes tested.

Reduced control on the IC life-cycle emphasizes various security issues associated with ICs. Hence, security of hardware ICs has emerged as a major challenge in IC design and test.

The main goal of the research is to develop design techniques that can effectively resist or mitigate the security threats at untrusted stages of the IC life-cycle. The main principle of the proposed techniques is design obfuscation method to achieve hardware security. In the work we consider the reconfigurable-based obfuscation in the post-fabrication stage of IC. We address the need to add reconfigurable-logic stage to the development cycle. This technique may be considered as a preventative measure concealing some of the design from an attacker. In other words, it hides the exact functionality and schematic of an IC until after the reconfigurable logic has been programmed.

Secure systems designing has been investigated earlier in diverse contexts. Previous works on protection of information systems can be broadly classified into two main categories [1-2]: embedding security mechanisms (access control mechanisms) at various levels of IS; multi-level Kernel-based security architecture.

In the work, the concept of multi-level kernel-based security architecture is considered.

Hardware obfuscation is a technique by which the description or the structure of electronic hardware is modified to intentionally conceal its functionality, which makes it significantly more difficult to piracy. In other words, hardware obfuscation modifies the design in such a way that the resulting architecture becomes unobvious to an adversary [3].

In this work reconfigurable logic-based obfuscation technique exploits reconfiguration features to obfuscate a design [4]. It suggests making a small component of the design reconfigurable in the IC. This approach hides the functional and/or schematic details in untrusted stages of the development cycle.

II. REFERENCE MONITOR OBFUSCATION

A basic concept in the design and development of secure systems is the concept of a reference monitor (RM) – reference validation mechanism.

A RM is an access control concept of an abstract machine that mediates all accesses to objects by subjects [5]. The RM allows developers to integrate the security aspect closer into design process of the system instead of trying to add it later.

The work is devoted to the RM obfuscation, ensuring the key property of RM: the RM must be non-bypassable.

In [6] the authors demonstrate formal transformations of the system structure model using multilevel aggregation. In this work we apply formal transformations approach for the RM obfuscation.

A complex system S is divided into the subsystems S_μ, where $\mu = 1, 2,..., M$. It is obvious that the subsystem S_μ, on the one hand, can itself be a complex system, just like the system S, and on the other hand, it can be an element of the system S.

The system under consideration S consists of 13 elements. The aggregation of the system is realized as follows: $S_\mu=\{C_1,C_2\}$ and $S_{\mu 0}=C_0{}^\mu=\{C_0,C_3 - C_{12}\}$. We assume that the subsystem S_μ will perform the access control functions, in other words, it will be the RM of the system.

The considered obfuscation method of RM consists of two steps. First step consists in construction of the operators (R_μ and $R_{\mu 0}$) of elements connections for the subsystem S_μ and $S_{\mu 0}$. The operator R_μ contains information associated with the connectivity of the RM (S_μ) and the main design ($S_{\mu 0}$). The second step consists in utilization of R_μ for reprogramming the subsystem S_μ at later stages of the design. Practically, we hide the functionality and schematic details of RM.

Proposed method of secure system design involves the access control mechanism as an obligatory element; the obfuscation of RM ensures the nonbypassable property of the access control mechanism; the formalism used in the work allows to automate a secure system design and mathematical

modeling to evaluating its resistance against various forms of attacks.

III. PHYSICAL IMPLEMENTATION

The application of the reconfigurable-based obfuscation of RM for SoC is as follows. The idea of utilization of R_μ for reprogramming the subsystem S_μ at later stages of the design is implemented of in the frame of FPGA platform. The work illustrates the use of reconfigurable feature of the Xilinx Vivado Design Suite and Nexys4-DDR board for obfuscate RM of SoC.

IV. CONCLUSION

In this paper, we have presented the approach that incorporate hardware design obfuscation to protect a design against various forms of attacks. The reference monitor obfuscation is performed using the multilevel aggregation algorithm of the structural model transformation. In order to obfuscate a reference monitor, our approach requires runtime field-programmable hardware features.

REFERENCES

[1] M. Bishop, Computer Security: art and science, Addison Wesley, ISBN 0-201-44099-7, 2002.

[2] C. Pfleeger, S. Pfleeger and J. Margulies, Security in Computing, Fifth Edition, Prentice Hall, pp. 1043, 2015.

[3] A. Sengupta, D. Roy, S. Mohanty and P. Corcoran, “DSP design protection in CE through algorithmic transformation based structural obfuscation,” IEEE Transactions on Consumer Electronics, vol. 63, no. 4, pp. 467–476, 2017.

[4] D. Forte, S. Bhunia and M. M. Tehranipoor, Hardware Protection through Obfuscation, Springer International Publishing, 2017 (Chapter 2, Fareena Saqib and Jim Plusquellic, VLSI Test and Hardware Security Background for Hardware Obfuscation).

[5] J. Anderson, “Computer Security Technology Planning Study,” Technical Report ESD-TR-73–51, Electronic Systems Division, Hanscom Air Force Base, Hanscom, MA, 1974.

[6] V. Gorbachov, D. Sytnikov, O. Ryabov, A. K. Batiaa and O. Ponomarenko, “Dimension Reduction for Network Systems Using Structure Model Aggregation,” International Journal of Design & Nature and Ecodynamics, vol. 15, no. 1, pp. 13–23, February 2020.

DOI: https://doi.org/10.30837/IVcsitic2020201356

Advantages of DNS-over-HTTPS over DNS

Hrushak Serhii[1]
[1]National Aviation University, 56 Zodchykh street, Kiev UA-03162, Ukraine, sg.grusha@ukr.net

Pavlenko Cynthia[2]
[2]National Aviation University, 56 Zodchykh street, Kiev UA-03162, Ukraine, neesmu13@gmail.com

Abstract. *Today information security concerns stand as the main topic in many computer-related fields. This work describes new standardized protocol: DNS-over-HTTPS. Encryption of DNS queries, pros and cons of new protocol, should we prefer DNS-over-HTTPS or just use old DNS? Let us try to figure it out.*

Keywords: *network; transmission of data; encryption of data; security; DNS; DNS-over-HTTPS.*

I. Introduction and Problem Statement

Domain Name System (DNS) – simple query-response protocol. Its main purpose is to name computers, services and other resources that connected to the Internet or private networks [1]. It translates human-readable domain names to corresponding IP addresses and so locates computer services with the underlying network protocols.

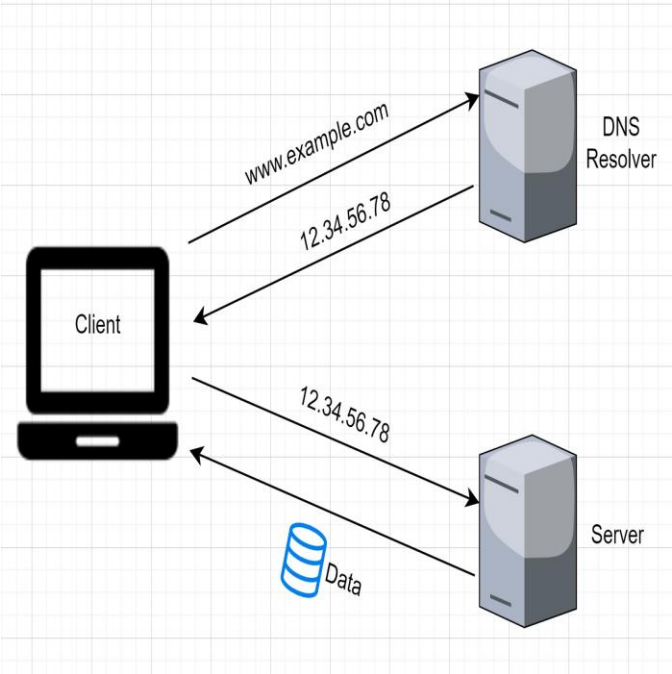


Figure. 1. Domain name resolving via DNS protocol

Nowadays, flow of data between computers constantly increases. As a result, needs in secured data transmission channels between them also increase. Theft of sensitive and private information can be disastrous for any private person or company. They may not even know that they use DNS every day, which does not determine the proper protection when transferring queries over Internet.

This work will tell about DNS-over-HTTPS protocol and its advantages over classical DNS.

II. Problem Solution and Results

DNS-over-HTTPS – is a protocol for performing remote domain name resolving via the HTTPS protocol [1]. Main goal of protocol is to increase user privacy and security by preventing eavesdropping and manipulation of DNS data by man-in-the-middle attacks (MITM). MITM attack is active eavesdropping, in which attacker creates independent connections between client and remote service, in that way relaying messages between them to make them believe that they are talking directly to each other over a private connection [2]. Such interconnection layer (man-in-the-middle) can read and change any data that goes through.

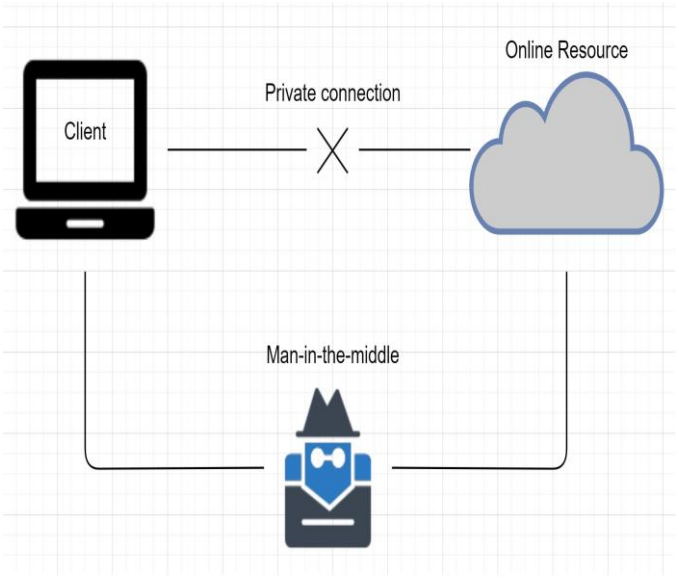


Figure. 2. Basic concept of man-in-the-middle attack

DNS-over-HTTPS requests/responses are handled over standard SSL port – 443. Protocol allows using two methods of HTTP requests: GET and POST. When using POST method original DNS query must be placed in body section of the message. Content-Type request header field must indicate the media type of the message. Protocol defines a new Content-Type request header for this – *application/dns-message*. Queries exchange between client and DNS-over-HTTPS server can be cached accordingly to HTTP and/or DNS basic cache rules.

Encryption of DNS-over-HTPS queries are done “on-fly” right before transmitting data between endpoints. Basic concept behind this procedure is beforehand established SSL connection between client and DNS-over-HTTPS server. SSL connection begins at handshake, which goals are to satisfy that client talks to the right server and vise-versa; agree on using encryption algorithm they will use to exchange data; agree on necessary keys for chosen algorithm [3]. After establishing SSL connection, client encrypts data before transmitting it to the server and vice-versa.

Let us review some pros and cons of DNS-over-HTTPS protocol. Pros are: makes MITM attacks useless; obfuscated data can't be sniffed by third-parties; all data flow is done using traditional SSL 443 port, so DNS queries can't be distinguished from traditional HTTPS queries; DNS traffic is centralized on a few DNS-over-HTTPS servers that may lead to improved load time performance. Cons are: makes traditional DNS-filtering practically useless; is not widespread today, so it lacks support [4]; decreases overall Internet cyber-security, because it makes harder to monitor suspicious activity [5].

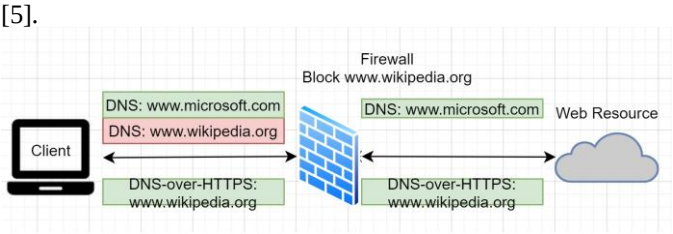


Figure 3. Firewall DNS-filtering outflank

III. Conclusions

DNS-over-HTTPS protocol closes Internet web-browsing security gaps by introducing encryption between DNS-clients and DNS-resolvers. Protocol intends transmitting queries over common HTTPS protocol and works with its standard rules.

As any new technology or protocol, DNS-over-HTTPS traditionally solves some problems and brings new ones. But one can be said for sure: it can become a new de-facto standard for DNS-resolving in the near future.

References

[1] Adam Roach, Benjamin Schwartz, RFC 8484 - DNS Queries over HTTPS (DoH), 2018, p. 21.

[2] Richard Chirgwin, IETF protects privacy and helps net neutrality with DNS over HTTPS, 2017.

[3] A. Freier, RFC 6101 - The Secure Sockets Layer (SSL) Protocol Version 3.0, 2011, p. 67.

[4] Lawrence Abrams, Google Unveils DNS-over-HTTPS (DoH) Plan, Mozilla's Faces Criticism, 2019.

[5] Zack Whittaker, Internet group brands Mozilla 'internet villain' for supporting DNS privacy feature, 2019.

DOI: https://doi.org/10.30837/IVcsitic2020201357

Intellectualization of information and communication systems vulnerabilities validation process

Kyrychok Roman

State University of Telecommunications, 7 Solomenska street, Kiev UA-03110, Ukraine, kyrychokr@gmail.com

Abstract. *The paper proposes a new approach to the intellectualization of information and communication systems vulnerabilities validation process during the active analysis of their security, the interconnection of the tasks of validating vulnerabilities, namely the tasks of verifying and confirming the possibility of implementing detected vulnerabilities through exploits and delivering the corresponding payload, with reinforcement learning is established.*

Keywords: *information and communication system; security analysis; validation of vulnerabilities; exploit, reinforcement learning.*

I. Introduction and Problem statement

Currently, one of the most common vectors of attack remains cyberattacks using software and hardware vulnerabilities. Their implementation is possible mainly through certain "operational" gaps that arise during the operation of information and communication systems as a result of administrative errors or untimely software updates or installation of additional patches, moreover, in the absence of a regular audit of information security, vulnerabilities may remain "uncovered" for years. Along with this, the threshold for entering the cybercriminal segment is reduced due to the automation of vulnerability exploitation tools, the availability of open databases, that are almost ready for use, exploits (Exploit Database, Inj3ct0r and others) and even entire exploit packs (Magnitude, Underminer, Purple Fox and others), which can easily be found and purchased on the darknet and conduct with them full-fledged cyberattacks on the infrastructure of target organizations.

Under such conditions, the use of preventive security methods, including active security analysis, remains promising, allowing not only to identify vulnerabilities but also to validate them, i.e. to confirm that a particular vulnerability can be realized, thus establishing an actual level of information systems and networks security.

To minimize the main drawbacks of active security analysis, namely, reducing the requirements for the qualification of experts and routine analysis itself, which is especially important for large networks such as corporate networks, where may be thousands of vulnerabilities, resort to automation and intellectualization of the validation process of found vulnerabilities. However, after analyzing these approaches [1-3] it should be noted that their effectiveness remains low, because:

- automation occurs mainly due to the sequential verification of vulnerabilities by the means of exploitation, i.e. through sequential launching of all selected exploits, taking into account simple criteria (operating system family, service, exploit rank and others). At the same time, it should be noted that most of them do not work, which indicates that the decision to use the selected exploit is false; moreover, the implementation of an incorrectly selected exploit in general can lead to complete failure of the target system;
- intellectualization is carried out through the use of classical methods of machine learning (training with and without a teacher), while leaving open the issue of obtaining quality data for training such systems.

The most promising solution to these problems may be the use of the reinforcement learning. Since the reinforcement learning itself is used in cases the machine needs to correctly perform the tasks assigned to it in the external environment, having many possible options for action and the ability to interact with this environment in real time.

II. Problem solution and Results

The reinforcement learning was developed in the works of R. Sutton and E. Barto [4] based on the theory of adaptive behavior developed by M.L. Tsetlin [5]. At the same time, it should be noted that in the method of reinforcement learning, concepts such as agent, environment, and reward are introduced, that directly describe the process of optimization of a certain task. The general scheme of the reinforcement learning process is shown in Fig. 1., which shows the interaction of the agent with the environment in discrete moments of time $t = 0,1,2\ldots T$, which are also called steps. The agent is some autonomous system, which has the ability to obtain information about the state of the environment (situation) and to affect through certain actions, which lead to changes in the situation. This means that the environment is an object or everything outside of the agent with what it interacts.

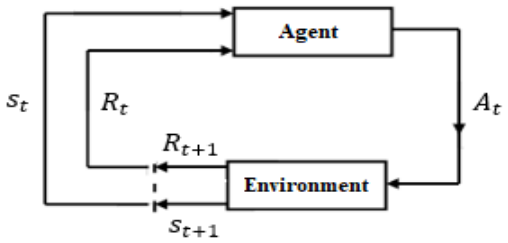


Figure 1. The general scheme of the reinforcement learning process [4]

At each time step t the agent gets a certain view of the state of environment $S_t \in S$, where S – is the final set of all possible states, and on the basis of this view selects the action $A_t \in A(S_t)$, where $A(S_t)$ – the finite set of actions that are available to the agent in the state S_t. In the next step, as a result of its action, with the help of evaluative feedback, the agent receives numerical reinforcement $R_{t+1} \in R \subset \mathbb{R}$, which can be both positive, $R_t > 0$ (reward), and negative, $R_t < 0$ (penalty), on the basis of which it forms a certain idea about the optimality of the choice made and finds itself in a new state S_{t+1}.

Thus, the agent that is learning has no input data about the need to perform a specific, predetermined "correct" action at a certain stage, moreover, it is often assumed that it does not even have any initial idea of the properties of the environment with which it interacts. On the other hand, the agent is able to make its own decisions about the choice of an action, by trial and error, to obtain reinforcement values, evaluating the performed actions and gradually improving its knowledge about the environment with which it interacts.

The main interconnection between the tasks of vulnerability validation, namely, the tasks of verification and confirmation of the possibility of implementing the discovered vulnerabilities through the use of exploits and delivery of the corresponding payload with the theory of reinforcement learning can be expressed as follows (Fig. 2):

- the vulnerability exploitation (validation) tool ↔ the agent;
- selected exploits of target information system vulnerabilities ↔ a set of action A;
- the validation tool chooses a vulnerability exploit and implements it ↔ the agent chooses and performs a certain action;
- the validation tool received the result of an attempted operation by revoking the target system ↔ the agent received numerical reinforcement for the performed action.

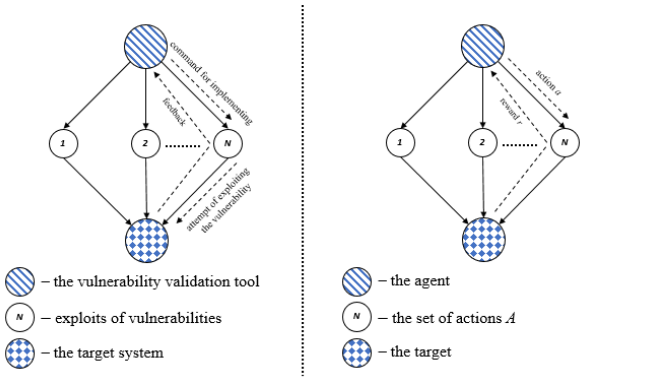


Figure 2. Relationship between the Vulnerability Validation tasks (left) and the Training task with Reinforcement (right)

Thus, it follows from the above that during the intelligent validation of vulnerabilities, exploits are ordered and implemented. During this process, the validation tool chooses the next exploit from the list of available ones (i.e. theoretically corresponding to the target system) and, by default, tries to execute it, waiting for the response from the target system and numerical reinforcement for the selected exploit. Based on this, it evaluates the optimal decisions made to use a particular exploit.

III. CONCLUSIONS

The proposed approach to the intellectualization of the vulnerabilities validation process of information and communication systems based on the use of the reinforcement learning will optimize the sequence of exploitation of likely vulnerabilities of software and hardware platforms in the target system, as well as reduce the percentage of false decisions on the use of selected exploits.

REFERENCES

[1] J. Luan, J. Wang, M. Xue, “Automated Vulnerability Modeling and Verification for Penetration Testing Using Petri Nets”, ICCCS (2), pp. 71-82, 2016.

[2] D. Wu, Y.-F. Lian, K. Chen, Y.-L. Liu, “A security threats identification and analysis method based on attack graph”, Jisuanji Xuebao (Chinese Journal of Computers), vol. 35, n. 9, pp. 1938–1950, 2012.

[3] C. Sarraute, “Automated attack planning”, Ph.D.thesis, School of Engineering, Buenos Aires, Argentina, July 2nd, 2012.

[4] R.S. Sutton, A.G. Barto, “Reinforcement Learning: An Introduction second edition”, The MIT Press, Cambridge, MA, 2018.

[5] M. L. Tsetlin, “Automaton Theory and Modeling of Biological Systems”, Academic Press, New York, 1973.

DOI: https://doi.org/10.30837/IVcsitic2020201358

Analysis of correlation rules in Security information and event management systems

Sievierinov Oleksandr[1]

[1]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, oleksandr.sievierinov@nure.ua*

Ovcharenko Margaret[2]

[2]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, marharyta.ovcharenko@nure.*

Abstract. *This article discusses the main components of information security systems and information security incident management. The methods of non-signature, as well as signature analysis of rules and decision-making that are used in such systems are considered. The analysis of existing methods of correlation rules. The main types of each method have been identified.*

Keywords: *correlation, information security management, signature method, non-signature method, incident security, event security, SIEM.*

I. INTRODUCTION

With an ever increasing amounts of information being processed in various information and communication systems in the first place come the availability of the tool with which it was possible to analyze events in real time. Because of the vast amounts of data to be processed is difficult to focus on the important aspects of information security company [6]. One solution is to use a Security information and event management system (SIEM) [1]. Base SIEM system is that data security incidents collected from various sources and the result of their treatment is given in a single report, which facilitates handling the incident and the decision to reduce the residual risk and losses [8]. The system SIEM consists of two segments - Segment Information Security Management (SIM), which is responsible for analyzing data to improve system efficiency and segment management of security incidents (SEM), with total media chooses the one with which incidents can be detected immediately [2].

Today SIEM system is one of the most common tools of analysis of information security incidents, so essential to clearly and correctly determine the rules by which your system will determine which event is incident and which - the result of the normal operation of the system, process or user. This article will discuss and analyze the main types of correlation method in SIEM systems and identify the basic methods that may be optimal for use in the design phase of SIEM systems.

II. CORRELATION OF EVENTS IN SIEM SYSTEMS

An information security event is an identified case of system or network status that indicates a potential breach of information security policy or security failure, or a previously unknown situation that may be material to the security policy.

An information security incident is a single event or a series of unwanted and unanticipated information security events that could result in business information being compromised and information security threats.

SIEM is a software solution that collects and analyzes data from many sources. The SIEM system collects data from network devices, servers, network event logs, antivirus software, firewalls, and other information security incident management systems, such as Data Leak Prevention (DLP) and Intrusion Detection System/ Intrusion Prevention System (IDS/IPS) [3]. SIEM stores, normalizes, applies to data that will be obtained from sources in previous stages, analytics that help identify events and information security incidents.

In practice, the circuit is implemented using the appropriate components[4]:

1. Agents (collecting data from various sources);
2. Collector servers (accumulation of information received from agents);
3. Database server (information storage);
4. Correlation Server (information analysis).

Correlation methods are used to more effectively process data and identify events in the information and telecommunication system as incidents of information security.

The correlation rules in SIEM systems are created using the following algorithm:

1. The target for which correlation will be performed is selected.
2. Information security events and conditions are selected.
3. The sequence of events is adjusted.
4. Specifies the time interval during which the event should occur.
5. A new rule is established.

There are two types of correlation methods in SIEM. The first type includes methods called signatures. These methods can be adjusted by the system user. The second type includes non-signatures, that is, those that independently detect security incidents and ensure their fixation and processing, which is used in most SIEMs.

There are many non-signature analysis methods. Usually the following methods are used in practice [6]:

1. Statistical - a method that essentially uses measurements of two or more variables and defines a statistical relationship between them.
2. A rule-based or template-based method is a method used to determine the cause-and-effect relationship of a rule that has been previously defined by administrators.
3. Graph-based method - correlation is performed by finding the dependence between the network components and plotting it as a graph. If component dependency was found, then the graph is used to find the events that caused this information security incident.
4. Neural Network Based Method - Correlation occurs by teaching neural networks to distinguish between information

security events and incidents and to perform certain actions that should minimize or even eliminate the risks to the system.

5. Codebook-based Method - Correlation occurs using vectors that fit from a predefined event matrix.

Despite the variety of non-signature methods, there is no way to overcome their major drawback. As non-signature correlation methods are developed and implemented by SIEM system vendors, the end-user is unable to make changes to their implementation, leading to a greater shift away from non-signature methods toward signature ones.

Signature methods are more flexible and effective for use in modern software implementations than non-signature methods [4]. The following notation is introduced to explain the operation of the signature methods:

1. P - problem, incident.
2. C - cause.
3. S - symptom.

An outline diagram of incident detection is shown in Fig. 1.

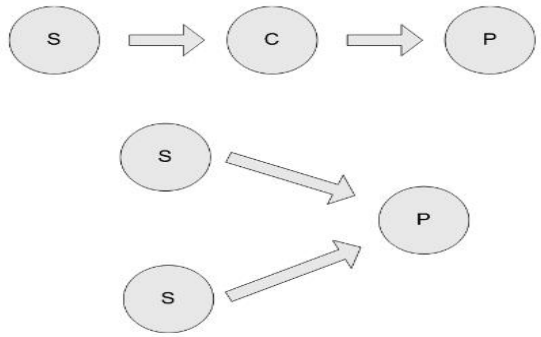


Figure 1. Diagram of information security incident detection

Signature methods are based on determining the criticality of an incident. There are two methods of determining it - quantitative and probabilistic. The quantitative method takes into account the number of symptom-cause-problem relationships. In the probabilistic method, each link is exposed to the likelihood of this symptom. Based on the sum of the corresponding probabilities, the criticality of the incident is exhibited [6].

The idea behind the signature method is to find matches with predefined correlation rules, each designed to identify and counteract a particular information security event, but several different rules can be triggered for each information security incident.

The rule includes a trigger that has a condition, a counter, and scenarios that describe the system's response to an information security incident.

The counter is used to calculate matches according to the same correlation rule. The trigger is waiting for one of the conditions to be enforced to enforce one of the predefined rules. And after a certain period of time (resetting the session), the trigger returns to zero until the next condition.

III. CONCLUSION

Thus, the analysis identified the main methods that can be used to correlate rules in SIEM systems, which in turn allow for a more accurate and effective analysis and counteraction to information security incidents that occur in information and telecommunication systems and can lead to significant system damage.

It has also been identified that the use of SIEM systems results in reduced response time to information security incidents and consequently lowers the economic costs that an individual business or government may incur. All that has been said, leads to the fact that the use of SIEM systems with signature methods of defining correlation rules and responding to them, increases the controllability of information security systems.

REFERENCES

[1] H. Karlzen, «An Analysis of Security Information and Event Management Systems: The Use of SIEMs for Log Collection, Management, and Analysis.» January 2009

[2] Сєвєрінов О.В. Управління інформаційною безпекою згідно міжнародних стандартів / О.В. Сєвєрінов, В.І. Черниш, М.Є. Молчанова // Системи управління, навігації та зв'язку. – К: ДП «ЦНДІ НіУ». - 2011. – Вип. 4(20). – С. 250-253.

[3] Алексей Дрозд, Обзор SIEM-систем //SearchInform [Электронный ресурс] — Режим доступа. — URL: http://www.antimalware.ru/analytics/Technology_Analysis/Overview_SECURITY_systems_global_and_Russian_market

[4] Martovytskyi V.A. Модель мультиагентної системи збору та зберігання інформації / V.A. Martovytskyi, I.V. Ruban // Системи управління, навігації та зв'язку. Збірник наукових праць. – Полтава: ПНТУ, 2017. – Т. 6 (46). – С. 150-153.

[5] Олеся Шелестова. Корреляция SIEM. Сигнатурные методы //исследовательский центр Positive Research [Электронный ресурс] 2012. URL:http:// www.securitylab.ru/analytics/431459.php

[6] Борисов В. И., Шабуров А. С.О Применении сигнатурных методов анализа информации в SIEM-системах

[7] Ушатов В. Проблеми оперативного виявлення і реагування на інциденти інформаційної безпеки / В. Ушатов, О. Сєвєрінов // GLOBAL CYBER SECURITY FORUM. Матеріали першого міжнародного науково-практичного форуму – Х.: ХНУРЕ, 2019. – С. 104-105.

[8] Овчаренко М. Аналіз сучасних систем управління інформаційною безпекою та інцидентами безпеки / М. Овчаренко, О. Сєвєрінов // Проблеми інформатизації: Тези доповідей сьомої мужнародної науково-технічної конференції – Х.: НТУ «ХПІ», 2019 – С.102.

DOI: https://doi.org/10.30837/IVcsitic2020201359

Analytical Estimation Methodology of Compromising Emanations Level Using Monte-Carlo Method

Perepadia Viktoriia[1]

Zabolotnyj Volodymyr[2]

[1] *Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine,viktoriia.perepadia@nure.ua*

[2]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, volodymyr.zabolotnyi@nure.ua*

Abstract. *Based on the electromagnetic field theory and the Maxwell equations, the paper describes the physical content and the way of the compromising emanations propagation into the far zone. This allows finding the dependence and methods of influence on of the test signal parameters, which represents a plurality of electrical impulses, with the change in the field strength at the point of conducting reconnaissance at the input of the receiving antenna, namely, in the distant zone of the technical channel of information leakage at the expense of compromising emanations. The main attention is paid to the Monte-Carlo statistical test method, which is used to generate parameters of videotract signals, which determine its shape in the distant zone. Applying the Monte Carlo method for generating values and will allow reasonably to formulate the realization of random parameters of videotract signals for their correct use during the estimation of compromising emanations level and development of measures protection.*

Keywords: *compromising emanations, technical protection of information, information leakage, statistical test method, distant zone, Monte Carlo method.*

I. INTRODUCTION AND PROBLEM STATEMENT

The most dangerous mode of the personal computer operation, in terms of information leakage, is the mode of the image playback on the monitor screen. This is due to the principle of the video adapter work, which consists of specialized circuits for generating electrical signals for controlling the hardware part of the image playback. The main element, which generates a powerful compromising emanations signal, is an electrical circuit, the equivalent of which is the frame with electric current. Physical processes and phenomena, that occur in it, are described by the corresponding Maxwell equations [1].

For the development of effective protection means from information leakage through technical channels at the expense of compromising emanations it is extremely important to quantify the compromising emanations level of hazardous signals. Referring to the normative and technical document «TP EOT-95», the values of the indicator of information leakage through technical channels at the expense of compromising emanations are absolute values (at the boundary of the controlled zone) of the intensity of the electric and/or magnetic field. It is advisable to estimate the reconnaissance range precisely in a far zone, because the distance, to which electromagnetic waves propagate, can reach tens of meters, and a potential reconnaissance device can be situated exactly within the far zone.

Typically, the intensity of the electric and magnetic field is determined experimentally with the help of measuring equipment, or experimentally-analytically with the use of control equipment. Since these methods have a number of significant drawbacks, the purpose of the work is to develop precisely an analytical estimation methodology of the compromising emanations level of the test signal harmonics of a personal electronic computer videotract.

II. THE ESTIMATION OF COMPROMISING EMANATIONS LEVEL USING MONTE-CARLO METHOD

In the practice of information technical protection, compromising emanations studies are explored on the basis of test signals. As test signals in most cases a signal of the type "meander" is chosen, that is, the sequence of regular signals "pixel black/pixel white" (fig. 1).

The defining parameters of the test signal are pulse amplitude A, pulse length at half-amplitude level (fig. 1).

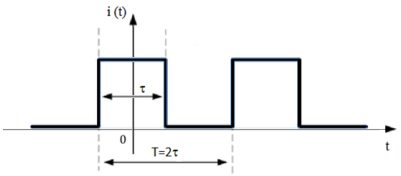


Figure 1. Signal of the type "meander"

In the previous paper [5], the way of determining the spectrum of a single pixel formation signal with the above characteristics is described. The method is based on the properties of the relations between the time and frequency characteristics of the signals during differentiation, integration, time shifting, scaling, based on the properties of Fourier transformations.

As a result of previous studies [6], it was found that in the distant zone, at the antenna input of the receiver, the shape of the explored compromising emanations signal is determined by the form of a second derivative from the form of the output electric current in the electric circuit circle of the video signal emitter in the form of the frame with electric current. In addition, the characteristic feature of the signals circulating in the real electrical circuits of the computer equipment, is the presence of such parameters as: δ is the length of the smooth transition of the signal between the linear parts (between the stationary value and the linear variable, and vice versa); Δ is the length of the approximation of the linear component of the pulse front (growth/decrease of the signal from *0* to *A*), which determine the shape of the signal. Moreover, there is an insignificant difference between smooth transitions bottom and top of pulses. The difference is due to the mechanism of their formation, namely the cutoff mode or the saturation regime, which are characteristic for the transistor operation of the pulsed circuits. The presence of the above parameters reduces

the radiation level of the signal at high frequencies [7]. This allows to minimize the compromising emanations level, thus providing the necessary level of information security. In turn, the pressing question remains the finding of the influence method on the values Δ and δ during the signal formation in the electrical circuit.

Since it is not always possible to determine the magnitude of the intensity of the electric field *E*, or its value is not accurate, the only correct approach for estimating technical protection of information is probabilistic. Its essence is to represent the desired quantities in the form of a range of values, that satisfy certain requirements.

The Monte Carlo method allows to solve probabilistic problems by statistical methods. The theory of this method indicates how to choose random values for calculations and how to evaluate the obtained results. The method is based on multiple runs (random implementations), based on the constructed model with the subsequent statistical data processing in order to determine the numerical characteristics of the object under study (process) in the form of its parameter's statistical estimates.

The imitation modeling by the Monte Carlo method allows to construct a mathematical model with uncertain parameters, and, knowing their probabilistic distributions, as well as the relationship between the change of parameters (correlation), obtain the distribution of the investigated function. Probabilistic distribution regulates the probability of choosing values from a certain interval. Within the model of the probabilistic risk analysis model, a large number of iterations are conducted to determine how a productive indicator behaves (within what range it fluctuates, what distribution) in the case of substitution of a variable in a model according to a given distribution.

For this, in the first place, it is necessary to model a sample of values Δ and δ , using Monte Carlo method within the specified limits. The distribution of values during the modeling is uniform, which ensures their greatest uncertainty. It is important to take into account some limitations associated with physical processes occurring in the computer equipment:

$$0 \le \delta \le \Delta \le \tau \,. \qquad (1)$$

Except the obvious inequalities (1), it is necessary to ensure the inequality implementation (2), which rejects such distortion of the simulated video pulses, that reduce their amplitude.

$$\delta \le \tau - \Delta \,. \qquad (2)$$

Generating of random values is carried out according to formulas (3) and is checked for compliance with restrictions (1) and (2).

$$\begin{cases} \Delta = \Delta_{\min} + \xi_1(\Delta - \Delta_{\min}), \\ \delta = \delta_{\min} + \xi_2(\delta_{\max} - \delta_{\min}), \end{cases} \qquad (3)$$

where $\Delta_{\min}$ is the value of the length of the approximation of the linear component of the pulse front, it is determined by the characteristics of the semiconductor components of the electronic circuit videotract;

$\delta_{\min}$ is the minimum value of the length of smooth transitions in the pulse, it is determined by the parasitic reactivity components of the electronic circuit videotract;

ξ_1, ξ_2 are the corresponding random variables values within 0-1.

Based on the foregoing, taking into account (3), the value Δ and δ should be situated in the selected region (fig. 2).

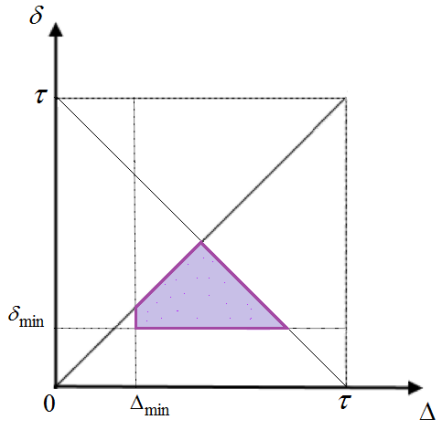


Figure 2. The region of values Δ and δ

III. CONCLUSIONS

As a result of the analysis, it was proposed the analytical estimation methodology of the compromising emanations level of the test signal harmonics of a personal electronic computer videotract. The described methodology has a number of advantages over the existing experimental ones. The obtained approach avoids obligatory activation of the computer equipment for the estimation of the information leakage technical channel, which makes it possible to scan compromising emanations before it is used. In addition, it is possible to assess the intelligence accessibility of computer equipment before it is manufactured.

Further researches will be will be dedicated to the substantiation of certain values Δ and δ to optimize the spectrum of harmonics in a given frequency band in accordance with the standards of protection.

REFERENCES

[1] J. Jin, *Theory and computation of electromagnetic fields*. Hoboken: Wiley, 2015.

[2] T. Simpson, *Maxwell on the electromagnetic field*. New Brunswick, NJ: Rutgers University Press, 1997.

[3] S. Alessio, *Digital Signal Processing and Spectral Analysis for Scientists*. Cham: Springer International Publishing, 2016.

[4] V.I. Zabolotnij, Ye.V. Gerasimenko, V.I. Perepadya. "Doslidzhennya zmin formi signalu u kanali pobichnih elektromagnitnih viprominyuvan monitoru [Investigation of the signal shape change in the compromising emanations channels of the monitor]." *Radiotehnika*, no. 176, pp.116-121, 2014.(In Ukrainian)

[5] V.I. Zabolotnyj, E.V. Gerasimenko. "Transformaciya formy signala v kanale pobochnyh elektromagnitnyh izluchenij [The waveform transformation in the compromising emanation channel]", in *Materialy Shestnadcatoy mezhdunarodnoy nauchno-prakticheskoy konferenciyi «Bezopasnost' informacii v informacionno-telekomunikacionnyh sistemah»* [*Procceding of 16th International Scientiffic and Practical conference "Information Security in Information and Telecommunication Systems"],* 2013, 155-159.(In Russian).

[6] S. Alessio, *Digital Signal Processing and Spectral Analysis for Scientists*. Cham: Springer International Publishing, 2016.

[7] D. Mukhopadhyay and R. Chakraborty, *Hardware security*. Boca Raton, Florida: CRC Press, 2015.

DOI: https://doi.org/10.30837/IVcsitic2020201360

Agent-Oriented Approach to Detect Hardware Trojans

Rosinskiy Dmytro[1]
[1]Kharkiv National University of Radio-Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, dmytro.rosinskyi@nure.ua

Kazmina Darina[2]
[2]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, daryna.kazmina@nure.ua

Muratov Vadym[3]
[3]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, vadym.muratov@nure.ua

Abstract. *The presented work is devoted to the problems of hardware tabs and methods for their elimination using agent modeling. The work is based on the principles of building hardware and software systems using separate technologies of the Internet of things. Both software and hardware technologies are used in the work, which are combined among themselves with the help of intelligent agents acting as intermediaries, eliminators, keepers and models of software and hardware.*

Keywords: *hardware trojans, agent modeling, intelligent agents, hardware and software systems, Internet of things.*

I. Introduction and Problem Statement

In recent years, new potential security threats in the field of electronics and programming based on hardware – the so-called hardware tabs or hardware Trojans, which represent a deliberate malicious modification of electronic circuits or structures, which leads to improper functioning of the electronic device. Being quite similar to a software tab, the hardware tab is a "black input" into the electronic device. This hardware Trojan has another additional advantage: it is always present at low levels of information processing, leading to conservation threats of failure or deviation from the normal operation of the system throughout the lifecycle of an electronic device, and the problem cannot be avoided by any software or hardware protection.

The range of hardware tabs (their capacities, sizes, operation mechanisms, power consumption) is huge, which together with the growing complexity of integrated circuits, both at the physical and functional levels provide ample opportunities for attackers to conceal hardware Trojans. Concerns about this hardware security issue are being expressed around the world, and it is believed that even more sophisticated and dangerous hardware tabs will be revealed in the foreseeable future [2, 5].

The purpose of the study is to model the behavior of hardware tabs and create means to eliminate and to detect them using agent-based modeling.

II. Problem Solution and Results

Using preventive approaches of warning and modern methods of detection of hardware tabs (the so-called hardware Trojans) does not give full guarantee that the manufactured software-hardware system is deprived of them [1]. As security threats are a large class and have a considerable number of states for the placement of hardware tabs, this has raised the issue of ensuring the safe operation of software-hardware systems with "infected" components, as well as the issue of correct prevention of activation of the Trojans. The very approach would allow using the equipment without paying attention to possible embedded Trojans. The experimentally studied and tested mechanisms of countermeasures [3] can be divided into two main groups (Fig. 1).

The first group of the mechanisms (including the processor commands) provides for preventing activation of the hardware Trojan and/or blocking the direct access of the Trojan equipment to any vulnerable data. The security device can control the sample data stored or transmitted within or between software and hardware systems of logic modules, blocking the mechanism by which the Trojan communicates with the data [2].

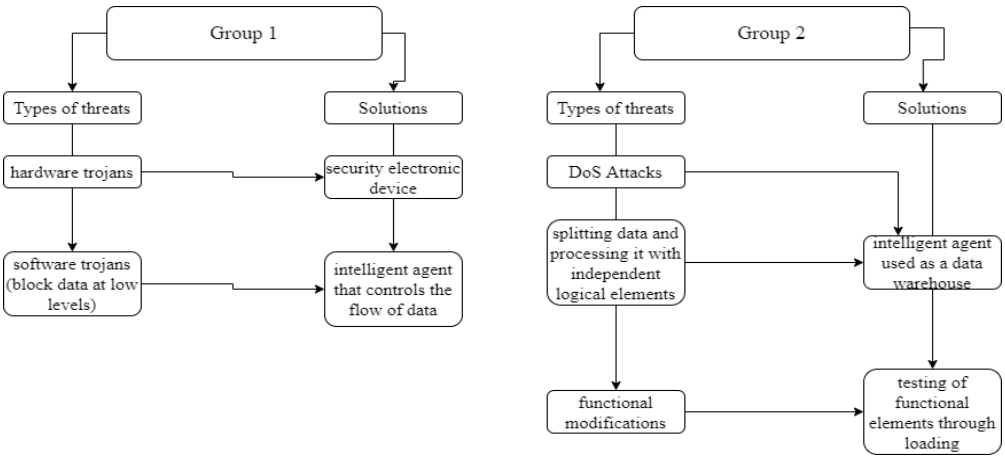


Figure 1. Classification of countermeasure mechanisms

The purpose of the intelligent agent in this group of methods is to monitor and adjust sample data to gather information about the behavior of individual logical components and send messages to the user about the "strange" behavior of the software and hardware system, or just send a list of problems caused by malfunction of logic module. To avoid getting a Trojan tab of the activation code there is another intelligent agent which holds scrambling the

performed the functions of the test elements that provided the loading. For example, in the course of the operation of a regular keyboard spy, the intelligent agent introduced by the hardware-software way simulated work with the keyboard, using it completely, during 6 hours.

Fig. 2 shows the fragment of code that is responsible for the operation of the keylogger. The result of this test was that a purposely created keylogger had run out of memory, and

```
public static void Logger (object sender, EventArgs e)
{
        if (!former.StolsClip.ToString().Contains(MyProject.Computer.Clipboard.GetText().
        Replace(''. '', ''<.> '').Replace       (''http '', ''<http> '')))
        {
                (!former.StolsClip = Operators.AddObject(former.StolsClip, MyProject.Computer.Clipboard.GetText().
                Replace(''.             '', ''<.> '').Replace(''http '', ''<http> '')
                + MyProject.Computer.Clipboard.GetText          ().Replace(''. '', ''<.> '').
                Replace(''http '', ''<http> '') + ''\r\n'');
        }
}
```

Figure 2. An example of shielding links used during keylogger

information channel [6-8]. Scrambling is used for processing data blocks that are not involved in the calculations. The principle of the agent is to encrypt selected data in a short time.

The second group is based on replication, fragmentation, and majority sampling strategies. This method is effective to protect against the DoS-attacks. The role of the intelligent agent in this method is to prevent the DoS-attacks by setting redundancy elements working in the project. Logic elements are subset into small pieces with little information. The intelligent agent or group of agents can be used as a data as a repository or their handler [3, 4, 5]. Accordingly, the data are grouped as fragments for storage and fragments for processing. At the same time there takes place a replication of selected pieces to ensure system reliability.

It is important to note that all the existing approaches to identify hardware tabs have its own unique features, but at the same time, there are some limitations. There is no method capable of detecting any class of malicious modifications with a high degree of certainty. The best way to improve the reliability of tests is to use the set of different ways to detect malicious software implementations and to provide comprehensive protection [1, 2, 4].

Hardware tab detection methods are divided into non-destructive and destructive ones. When destructive methods are used, the integrated circuits are demetallized to extract a layer-by-layer image of the chip using a scanning electron microscope.

Non-destructive methods can be divided into the system monitoring and testing prior to the system startup. In turn, the testing prior to the system startup includes two categories: the functional testing and the third-party channel analysis.

The system monitoring during its work is performed during critical calculations to detect specific harmful behavior that may occur during long-hour work. For example, a tab used to collect confidential information through wireless channels can cause large power surges during downtime.

Only non-destructive methods were considered in the article as they relate to both software and hardware. The intelligent agents involved in these methods performed work of "smart" observers (while monitoring the system performance, the intelligent agents observed the behavior of intentionally implemented hardware Trojan, making records stored on Google Drive, and sending work reports to the user), and work of "blockers" (i.e. they programmatically disabled the element that was affected by the Trojan).

During the testing prior to the system startup, the intelligent agents were involved in the functional testing. There, they strange messages indicating the location of the problematic component (the component was introduced into the system registry) began to arrive at the message center in the software that was created to manage the intelligent agents).

III. CONCLUSIONS

Since there is no solution that can provide comprehensive protection to the whole range of threats and mechanisms of activating hardware Trojans during hardware and software systems working, the combination of the existing classical methods (such as monitoring work of the system and functional testing) with the related fields (IoT, Cloud technology, machine learning) and new methods gives the highest efficiency. Using a combination of the methods presented can cover a wider area to detect and eliminate hardware threats. The latest technologies will allow not only conducting analysis by the standard tools in the usual places of damage, but will also be able to help detect hidden hardware tabs and create new methods for their elimination.

REFERENCES

[1] S. Bhasin, F. Regazzoni. A survey on hardware trojan detection techniques, In IEEE International Symposium on Circuits and Systems (ISCAS), 2015.

[2] H. Li, Q. Liu, J. Zhang. A survey of hardware Trojan threat and defense, 2016.

[3] Q. Sui, Z. K. Wu, J. Li, S. Q. Li. A detection method of Hardware Trojan based on two-dimension calibration. 2nd IEEE International Conference on Computer and Communications, 2016.

[4] J. He, Y. Zhao, X. Guo, Y. Jin. Hardware Trojan Detection Through Chip Free Electromagnetic Side Channel Statistical Analysis. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2017.

[5] C. B. Bao, D. Forte, A. Srivastava. Temperature Tracking: Toward Robust Run Time Detection of Hardware Trojans. IEEE Transactions on Computer Aided Design of Integrated Circuits and Systems, 2015.

[6] A. N. Nowroz, K. Q. Hu, F. Koushanfar. Novel Techniques for High Sensitivity Hardware Trojan Detection Using Thermal and Power Maps. IEEE Transactions on Computer Aided Design of Integrated Circuits and Systems, 2014.

[7] G. T. Becker, F. Regazzoni, C. Paar, W. P. Burleson. Stealthy Dopant level Hardware Trojans. International Conference on Cryptographic Hardware and Embedded Systems, ser. CHES. Berlin, Heidelberg: Springer Verlag, 2013.

[8] Martovytskyi V. O. Arkhitektura multyahentnoi systemy monitorynhu rozpodilenykh informatsiinykh system / V.O. Martovytskyi, K. R. Lokotetska // tezy dopovidei KhXVII mizhnarodnoi naukovo-praktychnoi konferentsii MicroCAD-2019, 15-17 travnia 2019 r.: u 4 ch. Ch. IV «Informatsiini tekhnolohii: nauka, tekhnika, tekhnolohiia, osvita, zdorovia». – Kh. : NTU «KhPI», 2019. – S. 164.

DOI: https://doi.org/10.30837/IVcsitic2020201362

Bluetooth vulnerability analysis

Samoilova Yana-Mariia

Odessa National Polytechnic University, Shevchenko Ave 1, Odessa UA-65063, Ukraine, yanamariyas1999@gmail.com

Annotation. *Attacks on personal data everyday become popular among hackers. Bluetooth is a kind of wireless network for file sharing between two devices, characterized by low cost, power, complexity and reliability, is a vulnerability to security protocols as well as user privacy. The purpose of the article is to analyze the shortcomings of Bluetooth security.*

Keywords: *information interception, vulnerability, hacking, Bluetooth, KNOB.*

I. Introduction And Problem Statement

In today's technical world, devices with Bluetooth technology are becoming increasingly popular. Users of gadgets and home appliances transmit a large flow of information every day. The more important and more confidential data, the greater threat of being intercepted by criminals.

Since the establishment of Bluetooth technology, many versions and bug fixes have been improved, but at the same time virus programs too. Bluetooth was developed as a cable replacement technology. This is a short-range radio intended for connecting portable electronic devices. There is a three-tier security control when transmitting data [1], but each system has its disadvantages. There are many applications, subroutines to control connection, such as[2]: MAC spoofing, Cabir Worm, BlueJacking, BlueSmack, BlueSnarfing, BlueBugging, Blueprinting, Blueover, BlueBorne, Fuzzing Attacks, Reflection attack, Backdoor attack, Denial of Service, Man-in-the-Middle/Impersonation Attack, War Nibbling, as well as distributions such as, Kali Linux, or a flash drive − MultiBlue Dongle. But one of the most active attacks that affect basically all devices - KNOB Attacks - is the topic of this article.

II. Problem Solution And Results

KNOB − Key Negotiation of Bluetooth[3]. The attack is possible due to the shortcomings in the Bluetooth specification that acts on the BR / EDR encryption key negotiation protocol. The attack allows a third party, without knowing the communication key or encryption keys, to force victims to match the encryption key only in 8 bits. The attack is hidden because the matching of the encryption key is transparent to Bluetooth users. As a result, the attacker completely breaches the security of Bluetooth BR / EDR by having access to personal data without being detected. Potential consequences may include charges for expensive calls, theft of sensitive information or malware downloads, full control of a connected "smart home" and tracking of user actions in online banking, keystrokes when transferring data between the wireless keyboard and the computer [4].

It was first discovered in 2018 by researchers at Singapore University of Technology and Design, as well as Oxford University's Computer Science Department, as a potential threat to users of any OS. Leading Bluetooth technology researchers was eliminating architectural vulnerabilities throughout the year. "We conducted KNOB attacks on more than 17 unique Bluetooth chips (attacking 24 different devices). … We were able to test the chips from Broadcom, Qualcomm, Apple, Intel and Chicony", says D. Antonioli (Singaporean University of Technology and Design) [5]. The study implemented the decryption of a file that is transmitted through an authenticated and encrypted Bluetooth connection at the link layer. A key with 1 byte of entropy leads to low costs, allowing the attacker to decrypt all encrypted text and enter other encrypted text even in real time. So, as a result, additional logic was plugged into the script to iterate over different CLK values (packets & clock metrics) and offset the E0 key stream. This basic logic only goes through the space of the encryption keys - 256 iterations [3]. Updated version Bluetooth 5.1 was introduced at the end of 2019, and all devices after 2018 that support this extension are safe.

III. Conclusions

The article deals with the dangers of Bluetooth encryption key negotiation protocol, which at first glance cannot pose such a threat, for example, when using headphones. This vulnerability has been skillfully identified and explored.

Developing upgraded versions of wireless communications has overcome data encryption gaps and security of use. The needs to analyze the technology, constantly study it, test it and improve it, are important factors for maintaining the privacy of users and, most importantly, their data.

References

[1] N. Be-Nazir Ibn Minar and M. Tarique, "Bluetooth Security Threats and Solution" A Survey. In International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January 2012.

[2] V. Tsira, G. Nandi, "Bluetooth Technology: Security Issues and Its Prevention" A Survey. In International Journal of Computer Technology and Applications (IJCTA) Vol.5, No.5, October 2014.

[3] D. Antonioli, N. Ole Tippenhauer, K. Rasmussen, "KNOB Attack. Key Negotiation of Bluetooth Attack: Breaking Bluetooth Security.", 28th USENIX Security Symposium, August 2019.

[4] M. Dinney, "McKenzie interchange Project – Travel Time Monitoring System: Technology Review", February 2016.

[5] D. Goodin "New Attack exploiting serious Bluetooth weakness can intercept sensitive data", August 2019.

DOI: https://doi.org/10.30837/IVcsitic2020201363

Modeling of information and cyber security cost optimization

Kononovich Vladimir[1]
Sievserinov Oleksandr[2]
Romanyukov Mykola[3]

[1]Odessa National Polytechnic University, 65044, Ukraine, Odessa, Shevchenko Ave. 1, kononovich@ukr.net
[2]Kharkiv National University of Radio Electronics, 61166, Ukraine, Kharkiv, Nauky Ave 14, oleksand.sievierinov@nure.ua
[3]Kharkiv National University of Radio Electronics, 61166, Ukraine, Kharkiv, Nauky Ave. 14, nikolay.romanyukov@gmail.com

Abstract. *The growing vulnerability of each individual in a progressive information and communication society is undeniable. Thus, on the part of the state, as well as the owner of the information to be protected, it is necessary to create new mechanisms that meet the modern requirements of individual protection of each subject of the system in information and cyberspace. This paper presents an effective method for calculating information and cybersecurity cost optimization. The class of societal attacks, which are identified as the most dangerous ones, is considered.*

Keywords: *information and cybersecurity; cost optimization; social engineering.*

I. INTRODUCTION AND PROBLEM STATEMENT

The significant development of progressive information technologies, combined with the communicative capabilities of the global digital "world", creates a number of grounds for regulating the security of these processes at the national and global level. The state information policy of Ukraine calls for new approaches to address information and cybersecurity issues, which is today the main component of national security and defense of the state [1].

The growing vulnerability of each individual in a progressive information and communication society is undeniable. Thus, on the part of the state, as well as the owner of the information to be protected, it is necessary to create new mechanisms that meet the modern requirements of individual protection of each subject of the system in information and cyberspace.

To date, the question of choosing the optimality criterion, taking into account the most dangerous class of attacks and a pessimistic strategy in modeling the process of optimization of information and cybersecurity costs, remains unresolved. Also, expert judgment is not taken into account when carrying out an information operation in terms of a measure of uncertainty that contains uncertainty.

The purpose of the work is to develop a method for optimizing information and cybersecurity costs. Identify the most dangerous class of information and cyber security attacks. Using subjective logic theory to account for uncertainty in estimates of possible costs by information and cybersecurity experts.

II. PROBLEM SOLUTION AND RESULTS

Formulation of the problem. To date, the question of choosing the optimality criterion, taking into account the most dangerous class of attacks and a pessimistic strategy in modeling the process of optimization of information and cybersecurity costs, remains unresolved. Also, expert judgment is not taken into account when carrying out an information operation in terms of a measure of uncertainty that contains uncertainty. Currently, there are several criteria for modeling the information operation process for the best possible pessimistic strategy: Laplace, Valda, Hurwitz, Bayes-Laplace and Sevid [2]. Using the priority of the choice of the decision in the absence of sufficiently complete information about the state of the system, in order to prevent excessively large losses, which can lead to the wrong decision, the criterion of the optimality of Sevid was chosen, which fully meets the requirements [3]. Using Sevid's optimality criterion, we propose a specific algorithm to solve the problem of information and cyber security minimization and introduce the following values: for the protection side, the Boolean variable $x_j \in \{0, 1\}, \ \forall_j \in M$ where $M = \{1,2..m\}$ multiple indices of remedies; $x_j = 1$ if $j-s$ protection will be used to protect against potential threats; $x_j = 0$ if $j-s$ no remedy will apply. Then $\vec{x}$ - the vector of boolean variables x_j ;for the attack side, the boolean variable $x_i \in \{0, 1\}, \ \forall_j \in N$ where $N = \{1,2..n\}$ – set of indices of means of attack; $y_i = 1$, if the party to the attack applies $i-s$ a means of attack; $y_i = 0$ if the attack is not applied $i-s$ a means of attack. Then $\vec{Y}$ – vector Boolean variables $y_i \,.\, V_{\max}(y)$ – the maximum possible damage from the implementation of attacks without the use of remedies for the defense party; $V_{biasted}(X,Y)$ – damages to the defense party in the event of a biased application of its protective equipment; V_I – average losses from impartiality $i-s$ threats; P_{ij} - probability to prevent $i-s$ the threat from the attack.

The essence of the algorithm is to solve the problem with Boolean programming, so a guaranteed result is achieved in terms of damage from attacks by defense. The algorithm that allows solving problems in Boolean programming corresponds to the method of implicit search on a vector lattice by the rule "1 dominates 0" [2]. Maximum cost optimization by a given criterion is achieved by introducing the following restrictions, when real losses for the protection side can be represented in the form [2]:

$$V(\vec{X},\vec{Y}) = V_{\max}(\vec{Y}) - V_{ynep}(\vec{X},\vec{Y}) = \\ = \sum_{i\in N} v_i y_i - \sum_{i\in N} v_i y_i \max_{j\in M} \{P_{ij}, x_j\}, \quad (1)$$

The defense side tries to minimize these losses and maximizes the attack side, meaning we have a zero sum game.

Since the choice of remedies solves the problem of minimizing the potential damage from attacks by the attacker, the Sevid criterion is transformed into a minimum risk criterion:

$$\begin{matrix} \min_{X\in\Delta x} \to admiss. \max_{Y\in\Delta y} \to admiss. \\ [\max_{X\in} \to admiss. \forall(\vec{X},Y) - V(\vec{X},\vec{Y})] \end{matrix}, \quad (2)$$

The given formulation of the mathematical model of antagonistic play is considered in a separate example. Given that more than 70 percent of all information security breaches are due to the "human factor", social engineering capabilities are widely used to obtain information about the attack object needed to provide NMS to the cybersecurity system. The main threats of social engineering from undesirable leakage of information according to statistics from [4], possible losses for the period of eight months and the conditional costs of the male-male attackers to carry out appropriate attacks during this period, are given in Table. 1.

Table 1. Losses from socio-technical attacks and the cost of their implementation

№	Threats	Damage from unbiased actions, thousand UAH	Cost of realization of threat of attacker, thousand UAH
1	Email	600	120
2	Telephone connection	300	60
3	Trash analysis	50	12
4	Personal approach	40	10
5	Reversing social engineering	140	16

IV.

Email threats are effective in spreading phishing messages with destructive information content. Damage data depend to a large extent on the specific activity of the attacked object and is therefore arbitrary given that, in the case of unbiased defense actions, the costs of the defenders' side significantly exceed the costs of the attacker's side [2].

Table 2 shows the methods of protection against threats, which are given by their numbers in accordance with table. 1, the cost of their implementation and the likelihood of threat prevention in the span of eight months.

Table 2. Methods for protection against security threats, the cost of their implementation and the likelihood of preventing threats in the span of eight months

№	Methods of protection	Cost of implementation, thousand UAH.	Probability of threat prevention				
			Threat numbers (Table 1)				
			1	2	3	4	5
1	Legislative	20	0,1	0,1	0,2	0,5	0,1
2	Morally ethical	27	0,6	0,5	0,2	0,3	0,4
3	Organizational and administrative	20	0,7	0,6	0,0	0,0	0,3
4	Organizational and technical	17	0,6	0,5	0,1	0,0	0,3
5	Informational	25	0,7	0,6	0,4	0,3	0,4
6	Organizational and economic	30	0,1	0,1	0,5	0,4	0,1
7	Engineering and technical	32	0,1	0,1	0,5	0,2	0,1

The approximate prices are given in Table. 2 define the security system configuration for the information system, taking into account their functional features [2]. Taking into account the initial data table. 1 and 2, and using the Boolean programming algorithm, we obtain solutions for the security side $\vec{X} = \|0, 1, 1, 1, 1, 0, 0\|$ and for the attack side $\vec{Y} = \|1, 1, 0, 0, 1\|$. This means that the selected methods of protection by the numbers 2,3,4,5 from the table. 2 and attack methods 1,2,5 from table. 1. The solution of the problem is optimal for the defense side, as in the case of biased defense action it is possible to reduce by 2.2 times the expenses (89 thousand UAH) compared to the expenses of the attacker (196 thousand UAH) and with high probability to eliminate all possible threats to social engineering. Analysis shows that email is the most vulnerable to the user.

For greater visibility of the obtained results, we will plot graphically the protection costs in the case of impartiality $P_{i.c}$ and prejudices $P_{p.c}$ measures according to the attacker's expenses $P_{a.}$.For convenience, we plot graphs in the coordinate system of decimal logarithms $\lg(P_{i.c}; P_{p.c.})$ and $\lg P_{a.}$ and are presented in Fig. 1.

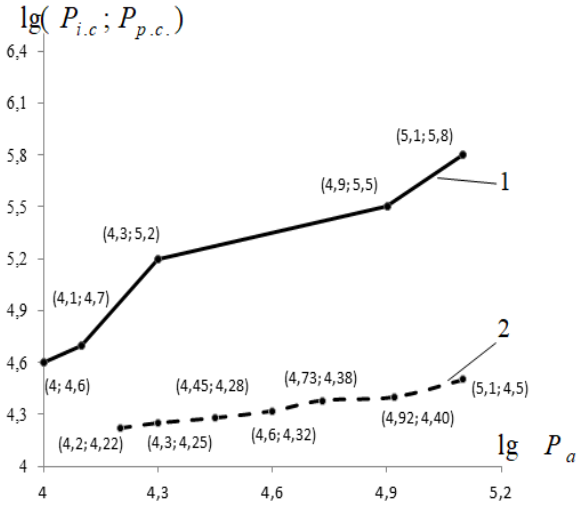


Figure 1. Loss dependency graphs $P_{i.c}, P_{p.c.}$ from social attacks $P_{a.}$: 1 – case of impartiality $P_{i.c}$ 2 – prejudices $P_{p.c}$

Graph 1 shows a significant increase in costs $P_{i.c}$ in the case of unbiased actions of the defender when the cost of the attacker increases $P_{a.}$. Graph 2 shows a significant reduction in costs $P_{p.c.}$ in the case of a biased application by the party of protection of the appropriate methods of protection (by numbers 1 - 7) according to the expenses in the unbiased actions of the defender $P_{i.c}$. Graphical dependence 2 corresponds to the optimal choice of methods of protection against social attacks.

For the right choice of optimal methods of protecting information with minimal cost, it is important to have a preliminary expert assessment of the possible risks in the conditions of certain uncertainty. Using Sevid's criterion, we construct a "risk matrix" for the above problem in order to make a decision that provides the minimum maximum risk value:

$$M = \left\| \begin{array}{cc|c} & & \max r_{ij} \\ 600 & 10 & 600 \\ 300 & 12 & 300 \\ 140 & 16 & 140 \\ 120 & 40 & 120 \\ 60 & 50 & 60^{*} \end{array} \right\|, \quad (3)$$

To the right of the "risk matrix" is the maximum risk column for each strategy A_i. Risk minimization is achieved when choosing a strategy A_5: 60 thousand UAH e-mail attacks.

The assessment of potential threats by information and cybersecurity professionals causes some uncertainty or uncertainty. The subjective logic theory (SL), developed by the Norwegian scientist A. Josang (Audum Jodsng), serves as an analytical description of such situations [5]. The centrality of subjective logic is the operation of three parameters. These parameters characterize the degree of trust (b), distrust (d), and uncertainty (u), provided that the true statement is arbitrary. The ability of SL theory to account for the uncertainty in the estimation of the possible costs by the defender, the possibility of interpreting its parameters, the presence of operators evaluating experts, makes it expedient to use it as an analytical apparatus. In this case, uncertainty is seen as filling the "vacuum" between trust and distrust. This situation can be mathematically expressed by the relation [5]:

$$\begin{array}{l} b + d + u = 1; \\ \{b, d, u\} \in [0,1] \end{array}, \quad (4)$$

One of the common tasks for information and cybersecurity is to determine the security of security features. To calculate a generalized opinion about the reliability of security remedies, it is necessary to use operators, the result of which is an opinion that confirms:

a) the belief in the simultaneous truth of the assertions concerning the reliability of all elements of protection;

b) the belief that one or more of the assertions regarding the reliability of the security features are true.

The following requirements are met by operators:

a) conjunctions of assertions;

b) the disjunction of assertions.

According to current views on information and cybersecurity, information and cyber security risk analysis is an integral part of information and cyber security activities.

At risk we will understand the product of the probability of carrying out the risk and the cash equivalent of the loss from the side of protection from its realization

To calculate subjective likelihood of risk, we use the statement conjunction operator, which is equivalent to the product of the likelihood of statements, if the opinions are dogmatic. The result of a conjunction operation is an opinion that is calculated on the basis of opinion W_X^A and W_Y some expert judgment A on the truth of the two statements X and Y and signifies a simultaneous belief in the truth of both statements.

The method of optimizing information and cybersecurity costs consists of the above advanced algorithm, as well as taking into account elements of subjective logic theory. In addition, subjective logic operates with a vector of thoughts that can be represented as a vector $W_p = \{b_p, d_p, u_p, a_p\}$. Vectors of thought are considered individually and necessarily belong to someone and belong to something. subjective logic operators are used to calculate the vectors of thought corresponding to expert judgment.

III. CONCLUSIONS

The method of optimization of information and cybersecurity costs is presented. The example of consideration of the attacker's socio-technical attacks shows the results of the defense party's cost calculations in the case of unbiased and biased actions. The use of Sevid's optimality criterion allows to set the minimum and maximum risks of monetary protection costs. E-mail has been shown to be the most vulnerable element in socio-technical attacks. Since in most cases, the interaction between the defense and the assault side takes place under uncertainty, expert attention is based on the theory based on subjective logic.

REFERENCES

[1] Stepanov V.Yu. Information security as a component of state information policy / V.Yu. Stepanov [Electronic resource] // State building. - № 2, - Kharkiv, 2016. - P. 525-542. - Access mode: http://www.kbuapa.kharkov.ua/e-book/db/2016-2/doc/1/02.pdf.J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[2] Bykov A.Yu. The task of choosing information protection tools in automated systems based on the antagonistic game model /A.Yu. Bykov, N.O. Altukhov, A.S. Sosenko. // Engineering Herald. - 2014. - No. 4. - S. 525–542.

[3] Abdenov A.Zh. The choice of means of effective protection using the methods of game theory / A.Zh. Abdenov, R.N. Zarkumova // Issues of information security. - 2010. - No. 2. - S. 26-31.

[4] Buryachok VL Information and cyber security: the social aspect: a textbook / [VL. Buryachok, VB Tolubko, V.O. Khoroshko, S.V. Tolupa]; for the total. ed. Dr. Techn. of Sciences, Professor VB Crowd. - K .: DUT, 2015. - 288 p.

[5] A. JosangAn Algebra for Assessing Trust in Certification Chains. InJ. Kochmar, editor, Proceedings of the Network and distributed Systems Security Symposium (NDSS'99). The Internet Society, 1999.

[6] Simonov S., Technologies and tools for risk management // Newsletter Jetinfo No. 2 (117), 2003. - S. 1-32.

DOI: https://doi.org/10.30837/IVcsitic2020201364

Prospects of information systems for detecting the propaganda texts

Tarasenko Yaroslav

Cherkasy State Technological University,
460 Shevchenko Blvd, Cherkasy, UA-18006, Ukraine,
yaroslav.tarasenko93@gmail.com

Abstract. *The work is devoted to searching the promising directions of developing the information systems for detecting the propaganda texts in order to increase the reliability of their functioning in the context of information confrontation and to ensure national security. As a result of researching the existing models and information systems for detecting the signs of psycholinguistic influence and propaganda, a promising direction of their development was found, which consists in applying the texts' automated classification. Based on the comparative analysis of information systems for morphological analysis in text categorization with the system for defining the morphological-syntactic and semantic category of the propagandist's psycholinguistic portrait, the perspective ways of developing the information systems for detecting the propaganda texts are determined.*

Keywords: *psycholinguistic influence, propaganda detection, automated texts' classification, semantic category, quantum-semantic study.*

I. Introduction and Problem statement

Today, more and more states are united in a single information space. In addition to the positive features, such as free experience exchange, quicker response in business, economics or politics, this phenomenon leads to introducing the concept of information warfare. Ukraine is also involved in information warfare, and based on [1], as no one else needs reliable tools to protect and counteract the usage of information weapons. The article also states that one of the means for conducting information war is purposeful informational influence on the population. It can be said for sure that this type of information weapon is one of the most dangerous. However, as noted in [2] there are subspecies of psychological weapons, such as information-psychological, linguistic, psychotronic, psychophysical, psychotropic and somatopsychological weapons. All types of informational-psychological weapons except the linguistic one are not difficult to detect due to the aggressiveness of the action and the inability to implement certain types in the information space. So, linguistic weapon is definitely the most dangerous.

There are modern information systems for detecting signs of information-psychological manipulation, based on models [3-4], which use different approaches to detect the influence on consciousness. However, even promotional text will have the following characteristics, but the real danger is the propaganda text. There are automated information systems for propaganda detection in textual data based on the transfer learning approach [5], or on the methods of propagandist's identification in the social network [6]. But a study of information systems for propaganda detection in textual data has shown that the mentioned above methods and information systems for propaganda detection are aimed at investigating the offender's behavior, identifying signs of misinformation, etc., and this is not sufficient for conducting a deep investigation of well-hidden propaganda that affects consciousness. Although all systems agree on a common approach which is in automated text analysis.

Therefore, there is a need to explore promising areas for the further development of existing information systems for detecting propaganda texts and, as a consequence, a need to develop approaches for their effectiveness and reliability improvement, in context of increasing danger from the information warfare and the national security providing as a whole.

II. Problem solution and Results

Improving the reliability of propaganda detection information systems is possible by improving the efficiency of automated text analysis. Since only semantic analysis can determine the hidden meaning and its perception by the target audience, research should be directed to a more comprehensive concept of automated textual analysis, namely, automated text classification [7], which includes automated morphological or semantic analysis of textual information, as well as the syntactic and emotional analysis used in the mentioned models and systems of detecting the propaganda.

In addition, the article [7] presents the experimental analysis results of various automated information systems for classifying texts which are based on diverse approaches to the terms' detection and classification, including English terms. However, the task of identifying the propaganda has its own specificity, which requires special look on analyzing the text. Particular attention is paid to known morphological analysis algorithms and the results are presented.

In turn, in [8] it was carried out the work on the use of quantum-semantic research in the text's formation or modification according to propagandist's individual semantic function. At the same time, the morphological-syntactic and semantic category of the propagandist's psycholinguistic portrait is considered.

In the course of the comparative experiment, an automated information system for determining the coordinates of the semantic particle was implemented and the results of the morphological analyzer functioning when automatically classifying the texts were compared with the study results of the morphological-syntactic and semantic category of the propagandist's psycholinguistic portrait. The experiment was based on a set of 50 texts with signs of psycholinguistic influence written by different authors. Special elements of information propaganda were added in 30% of the texts manually using the most common methods of both explicit and

covert propaganda. The results of the comparison are shown in the table 1.

Table 1. The characteristics of morphological analysis in text categorization compared with the morphological-syntactic and semantic category definition

Characteristics	Morph. analysis (in categorization)				Morphological-syntactic category				Semantic category	
Transaction time (sec)	0,5-3				2-5				15-45	
Text size (thousands of characters)	1		5		1		5		1	5
Number of tests	15	50	15	50	15	50	15	50	50	50
Accuracy of propaganda definition	23 %	20 %	31 %	29 %	48 %	45 %	64 %	61 %	79 %	87 %

The analysis has shown that categorization by morphological units is not accurate. However, there was no detected efficiency increase caused by changing the specific morphological analysis algorithm or by the experiments' number. The main difference is in the fundamental approach to text analysis and in the direction of the further research. Improvement of accuracy is possible on the basis of analyzing the semantic category, especially in the context of considering the propagandist's psycholinguistic portrait.

Thus, based on the experiment results, it is possible to note the following perspective ways of developing the information systems for detecting the propaganda texts, which are considered to be able to improve the reliability and efficiency of the automated process of information propaganda detection.

1. Conducting semantic research to provide a process of deep analysis and to increase accuracy in the automated categorization of propaganda texts, taking into account the types of propaganda activities.

2. The automated morphological analysis algorithms adaptation for taking into account the features of the propagandist's psycholinguistic portrait, as well as the text's propaganda discourse and the offender's psycho-emotional characteristics.

3. The quantum-semantic analysis usage for taking into account the quantum nature of the perception the word's forms as well as semantic categories, which improves the accuracy of detecting the hidden propaganda.

4. Replacing popular approaches of text analysis by the neural networks with faster computer hermeneutic systems that do not require a long and painstaking process of training the neural network, the essence difficulty of which is in selection and classification a core sample test.

III. CONCLUSIONS

For developing the approaches to improve the efficiency of information systems for the detecting the propaganda texts, as well as to increase their reliability considering the increasing risk of hostile psycholinguistic influence, it is proposed to increase the efficiency of information systems for automated text classifying in such areas as focusing on semantic analysis, retraining the algorithms of morphological analysis, using the quantum-semantic approach and applying the computer hermeneutics in complex in order to improve the reliability of textual data categorization considering the informational propaganda.

REFERENCES

[1] Malyk Ya. Information war and Ukraine / Ya. Malyk // Academic papers collection «Democratic governance», 2015. – Issue 15. URL: http://www.lvivacademy.com/vidavnitstvo_1/visnyk15/fail/Malyk.pdf

[2] Makarenko S.I. Information confrontation and electronic warfare in network-centric wars at the beginning of the XXI century / S.I. Makarenko: monograph. – St. Petersburg: High technology, 2017. – 546 p.

[3] Goncharov I.V. Modeling the processes of information-psychological impact in social networks / I.V. Goncharov, P.A. Parinov, A.A. Sirota // Proceedings of Voronezh State University. Series: Systems analysis and information technologies, 2018. – № 2. – P. 93-104.

[4] Java S. Detection of Online Manipulation to Prevent Users Victimization / S. Java, F.L. Basheer, S. Riaz, M.J. Kaur, A. Mushtaq // Proceedings of Amity International Conference on Artificial Intelligence, Dubai, UAE, February 4-6, 2019. – P. 593-599.

[5] Aggarwal K. NSIT@NLP4IF-2019: Propaganda Detection from News Articles usingTransfer Learning / K. Aggarwal, A. Sadana // Proceedings of the 2nd Workshop on NLP for Internet Freedom: Censorship, Disinformation, and Propaganda, Hong Kong, China, November 4, 2019. – P. 143–147.

[6] Orlov M. Using Behavior and Text Analysisto Detect Propagandistsand Misinformers on Twitter / M. Orlov, M. Litvak // Proceedings of the 5th International Conference «Information Management and Big Data», Lima, Peru, September 3-5, 2018. – P. 67-74.

[7] Batura T.V. Automatic text classification methods / T.V. Batura // Software and Systems, 2017. – Vol. 30, № 1. – P. 85-99.

[8] Tarasenko Ya. Determining the coordinates of semantic particle in english text with a known psycholinguist portrait of propagandist / Ya. Tarasenko // Ukrainian Information Security Research Journal, 2019. – № 21 (3). – P. 168-174.

DOI: https://doi.org/10.30837/IVcsitic2020201365

Method of the Increasing the Detection of Digital Radiosignals

Barabash Oleg[1]
Laptiev Oleksandr[2]
Svynchuk Olga[3]
Openko Pavlo[4]

[1]State University of Telecommunications, Solomenskaya Str., 7, 03110 Kyiv, Ukraine, Email: bar64@ukr.net
[2]State University of Telecommunications, Solomenskaya Str., 7, 03110 Kyiv, Ukraine, Email: alaptev64@ukr.net
[3]State University of Telecommunications, Solomenskaya Str., 7, 03110 Kyiv, Ukraine, Email: 7011990@ukr.net
[4]Ivan Cherniakhovskyi National Defense University of Ukraine, Povitroflotsky Prospect 28, 03049 Kyiv, Ukraine, Email: pavel.openko@ukr.net

Abstract. *In the process of detecting and recognizing a digital radio signal, a topical issue is increasing noise immunity. The features of the use of low frequency filters with quadratic and linear response dependence on the input signal are investigated in the article. It is shown that the principle of operation of filters is that the summation process is performed. In this case, the useful signal is summed up coherently and the interference signal is incoherent, ie, the useful signal increases and the interference signal decreases. The filtration process is simulated at different correlation coefficients. This confirmed the possibility of isolating the signal of the means of silent receiving of information by the method of determining the two-dimensional density of the likelihood of interference signal against the background of the common signal. It is proved that the use in the process of signal processing of narrow-banded filters of low frequency allows to increase the noise immunity of the system of detection and recognition of digital radio air signals by 23 %.*

Keywords: *noise immunity, filter, mathematical expectation, variance.*

I. Introduction and Problem Statement

A considerable number of publications are devoted to the issue of noise immunity. The technical methods of improving radio efficiency related to noise immunity are considered. However, noise immunity issues are not addressed when probable digital signals are detected. The issue of digital signal recognition is not resolved. From the analysis of modern literature, we can conclude that the problems of noise immunity, which have their own peculiarities in the process of detecting and recognizing digital signal of digital radio broadcasting, are practically not considered.

II. Problem Solution and Results

Almost all methods of noise immunity receive signals based on the principle of signal averaging and interference. This principle is that the summation process is performed. Moreover, the useful signal is summed up coherently, and the noise signal is incoherent. For the purpose of averaging the useful signal and interference, linear systems of two types are used: narrow band filters and low frequency filters. It is possible to optimize low pass filters or narrow band filters.

To consider the issue of interference filtering, let us assume that the narrowband filter itself does not distort the signal that has passed through it. An ideal bandpass filter is a filter with an amplitude-frequency response of the type:

$$K(\omega)=\begin{cases}1 \quad if \quad \omega_0-\dfrac{\Delta\omega}{2}\le|\omega|\le\omega_0+\dfrac{\Delta\omega}{2}\\ 0 \quad if \quad \left]-\infty,\omega_0-\dfrac{\Delta\omega}{2}\right[U\left]\omega_0+\dfrac{\Delta\omega}{2},\infty\right[\end{cases}, \tag{1}$$

The frequency response of the expression for (1) is the impulse transition characteristic, which will be determined by the expression:

$$h_\delta(t)=\frac{\Delta\omega}{\pi}\cdot\frac{\sin\dfrac{\Delta\omega t}{2}}{\dfrac{\Delta\omega t}{2}}\cos\omega_0 t \ . \tag{2}$$

Given that the digital signal is not a clear pulse [8], it is possible to calculate the envelope voltage at the output of an ideal filter when exposed to a rectangular pulse of duration:

$$x(t)=\begin{cases}X_m\cos\omega_0 t \quad if \quad 0\le t\le T\\ 0 \quad if \quad \left]-\infty,0\right[U\left]T,\infty\right[\end{cases} \tag{3}$$

Using the envelope voltage theorem of the narrowband filter, we write the expression for the envelope voltage at the output of the filter:

$$Y_m(t)=\frac{1}{2\pi}\int_{-\infty}^{\infty}K_{fn}(j\omega)S_{X_m}(j\omega)e^{j\omega t}dt \ . \tag{4}$$

$$K_{fn}(j\omega)=\begin{cases}1 \quad if \quad -\dfrac{\Delta\omega}{2}\le|\omega|\le\dfrac{\Delta\omega}{2}\\ 0 \quad if \quad \left]-\infty,\dfrac{\Delta\omega}{2}\right[U\left]\dfrac{\Delta\omega}{2},\infty\right[\end{cases}. \tag{5}$$

Substituting expression (5) into expression (4), we get the expression:

$$Y_m(t)=\frac{X_m}{2\pi}\left(Si(\Delta\omega t)-Si(\Delta\omega(t-T))\right). \tag{6}$$

In fig. 1 dependency graphs of the duration of the influencing rectangular pulse (blue color - pulse duration T = 1, red color - T = 10, green color - T = 15 and black color - T = 20) on the frequency range (filter bandwidth).

The graphs show significant differences between the input rectangular pulse and the output signal. The distortion of the input impulse increases as its duration increases. This distortion of the pulse shape can be characterized by the duration of the envelope of the impulse of the filter output to the duration of the envelope of the output impulse.

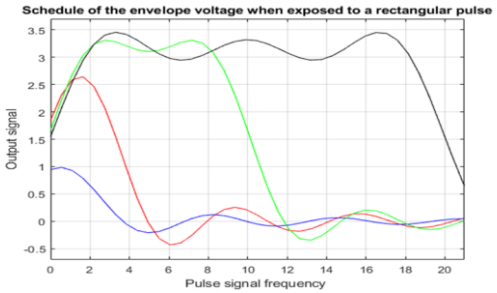


Figure. 1. Graph of the envelope voltage when exposed to a rectangular pulse signal

Research, methods and research techniques, collection and processing data, and for the mathematical and computer models - results of numerical simulations.

III. CONCLUSIONS

The peculiarities of the use of low-pass filters to increase the noise immunity of an automated system for detecting and recognizing digital airwaves are investigated. It is shown that the principle of operation of filters is that the summation process is performed. In this case, the useful signal is summed up coherently, and the noise signal is incoherent. That is, when summing up, the useful signal increases and the interference signal decreases.

Taking into account the peculiarities of the digital signal, the signal parameters are defined (mathematical expectation, correlation coefficient, variance, root mean square deviation) and the outputs of linear and quadratic filters at the influence on the input of a rectangular pulse that simulates the signal of modern digital means of silent receiving of information are determined.

The graphs of the envelope voltage at the output of the perfect bandpass filter with the influence on the input of a rectangular pulse (digital signal) of different duration are obtained.

The results of the simulation of the filtering process, with different correlation coefficients, confirmed the possibility of selection of the digital signal by the method of determining the two-dimensional probability density of the signal of interference on the background of the common signal.

It is proved that the use in the process of signal processing of low bandwidth filters of low frequency allows to increase the noise immunity of the system of detection and recognition of digital radio airwaves signals by 23 %.

A considerable number of publications are devoted to the issue of noise immunity. Thus, in [1], the technical methods of improving radio efficiency related to noise immunity are considered. The methods of increase of noise protection and noise immunity are considered and the factors that shape them. It is shown that variants of coding of the source of information do not fundamentally affect the stability of radio stations during the action of these interferences. However, noise immunity issues are not addressed when probable digital signals are detected. In [2], the process of noise immunity of a typical detection path composed of sequentially included modules is considered: an ideal bandpass filter, a quadratic detector, and an ideal integrator. However, the issue of the effect of interference on a rectangular signal that is similar to a digital signal is not addressed. In article [3], using the methods of statistical radio engineering, the noise immunity of receiving signals with quadrature amplitude modulation in the presence of noise and harmonic interference is analyzed. In article [4], based on distributed models, a method of bringing voice signals to a single amplitude and time window is proposed. The proposed methods can be used in signal recognition systems. In [5], an optimization model for the measurement of power in circuits was developed on the basis of studies conducted in MATLAB. In [6] investigated the effect of multiray propagation of radio waves on the transmission of audio content through channels with normal and lognormal interference distribution using GSM and WiMAX wireless technologies. In [7], a technique for the interaction of mobile technical objects in the process of data flow transfer under conditions of powerful electromagnetic field is proposed. The work [8] is devoted to increasing the noise immunity of information messages under the conditions of powerful electromagnetic interference by the use of complex signal-code structures. This increases the volume and speed of information transfer. In [9] the results of studies on increasing the signal-to-noise ratio in mobile communication systems are highlighted. This direction is realized through the use of methods of dynamic change of transmitter power, organization of multiple access and dynamic distribution of communication channels. However, the issue of digital signal recognition is not resolved. From the analysis of modern literature, we can conclude that the problems of noise immunity, which have their own peculiarities in the process of detecting and recognizing digital signal of digital radio broadcasting, are practically not considered.

REFERENCES

[1] Bakiko V.M., Popovich P.V,. Shvaychenko V.B. Viznachennya zavadostiykosti kanalu zv'yazku za vipadkovogo vplivu zavad. Visnyk Nats. tehn. un-tu "HPI" : zb. nauk. pr. . – Kharkiv : NTU "HPI", 2018. № 14 (1290). S. 7 – 10.

[2] Churyumov G., Tokarev V., Tkachov V., Partyka S. Scenario of Interaction of the Mobile Technical Objects in the Process of Transmission of Data Streams in Conditions of Impacting the Powerful Electromagnetic Field. 2018 IEEE Second International Conference on Data Stream Mining & Processing (DSMP). 21-25 Aug. 2018. P. 183 – 186.

[3] Fedorov E., Alrababah H., Nehad A. The distribution for mation method of reference patterns of vocal speech sounds. International Journal of Advanced Trends in Computer Science and Engineering. 2017. Vol. 6 (3), May - June, P. 35 – 39.

[4] Kulikov G.V., Nesterov A.V., Lelyuh A.A. Pomehoustoychivost priema signalov s kvadraturnoy amplitudnoy manipulyatsiey v prisutstvii garmonicheskoy pomehi. Zhurnal radioelektroniki, № 11, 2018 [Elektronniy resurs] Rezhym dostupu: https://elibrary.ru/contents.asp?id=36651217 (20.03.2020).

[5] Laptiev O.A., Barabash O.V., Savchenko V.V., Savchenko V.A., Sobchuk V.V. The method of searching for digital means of illegal reception of information in information systems in the working range of Wi-Fi. International Journal of Advanced Research in Science, Engineering and Technology. India. 2019. Vol. 6, Issue 7. P. 10101 – 10105.

[6] Laptiev O., ShuklinG., Savchenko V., Barabash O., MusienkoA., Haidur H. The Method of Hidden Transmitters Detection based on the Differential Transformation Model.. International Journal of Advanced Trends in Computer Science and Engineering. 2019. Vol. 8, №6, November- December. P. 538 – 542.

[7] Laptiev Oleksander, Savchenko Vitalii, Syrotenko Anatolii, Shchypanskyi Pavlo, Matsko Oleksander, International Journal of Innovative Technology and Exploring Engineering (IJITEE) Volume-9 Issue-4, February 2020. Scopus Indexed - ISSN 2278 – 3075. P. 2114 – 2119.

[8] Parkhomenko A.N., Shotskyi B.I. Pereshkodostiikist typovoho traktu pry vyiavlenni syhnaliv z fluktuatsiinoiu amplitudoiu. Mizhnarodnii naukovo-tekhnichnyi zhurnal. [Elektronnyi resurs] Rezhym dostupu: http://radio.kpi.ua/article/view/S002134701982040219 (14.11.2019).

[9] Serkov O. Breslavets V., Tolkachov M., Kravets V. Method of coding information distributed by wireless communication lines under conditions of interference. Advanced Information Systems. 2018. Vol. 2, No. 2. P. 145 – 148.

DOI: https://doi.org/10.30837/IVcsitic2020201366

Aspects of the development of the comprehensive information security system in the information systems

Nosyk Andrii[1]
[1]National Technical University "Kharkiv Polytechnic Institut", 22 Kyrpychova str, Kharkiv UA-61002, Ukraine, nampbch@gmail.com

Kucherenko Yurii[2]
[2]Kharkiv National Air Force University of Ivan Kozhedub , 77/79 Sumska str, Kharkiv UA- 61023, Ukraine,kucherenkoYF@gmail.com

Nosyk Kateryna[3]
[3]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, kateryna.nosyk@nure.ua

Abstract. *Here are considered some aspects on the comprehensive information security system development of any information system of civil purposes, which manages the critical infrastructure or process in a relevant field, or control systems for special purposes. The basis for the functioning of these systems is information, and because of it the issue of protection is paramount in their functioning. The questions on the choice of general security policy in them, the choice of methods for identification and authentication, authentication of documents, circulating them. This will conceptually define the future of information security records they elaborate.*

Keywords*: information, information systems, comprehensive information security system, method, unauthorized access, security policy,*

I. Introduction and Problem statement

Large-scale application of information systems (IS) in various sectors of society, including commercial activities, management of critical infrastructure facilities or systems of state management, military (air traffic control systems, automated control systems of nuclear power plants, and command and control facilities and other commercial systems) requires solving the issue of information security in them [1]. Information security in the IS aims to prevent access by unauthorized persons and various technical devices to electronic resources (data banks and knowledge banks) and information circulating in the system, for its copying, destruction or distortion. Access to information held in the IS by strangers can cause large economic losses and environmental and technological disasters, and therefore, to prevent these phenomena should develop robust information security system in IC for various purposes. Therefore, the proposed review of certain aspects to develop a comprehensive information security system (CISS) IS has particular relevance to the developer, the formation of different accounting systems to protect information that they have developed [2].

II. Problem solution and Results

The issue regarding the IS Security Policy different function is only possible through an integrated approach to sustainable use of software and hardware (software, hardware) protection and relevant information (including designation system) organizational and technical measures to be implemented in the CISS of a system [1-5].

The organizational measures directed staff to work with the relevant IS (organization of physical protection, responsibility for implementation of personnel protection, the monitoring of performance, protection measures) [3].

Technical (engineering) measures aimed at reducing the dangers caused by external factors influence the operation of the IS (natural disasters, man-made phenomenon, means fire destruction, etc.), providing the required level of survivability of the system and eliminate certain threats to information security through the use of different information security controls and security situation.

Software and hardware (software, hardware) methods provide protection against threats associated with the process of collecting, processing, storage, retrieval, communication system among its users [4-5].

It should be noted that the level of safety and reliability CISS will not only depend on the tools and measures selected for data protection and overall security policy but, in our opinion, and from an integrated application of these measures and methods to implement targeted effect of information security.

In developing CISS developers must firstly define information security policy, such as which methods of security policies to choose - discretionary or mandatory. The simplest method of constructing security policy is discretionary method of access to facilities. When using which the current random access Agent of subjects (users) to other objects IS (using the access matrix). Credentials method of access to facilities using tags matching security levels of subjects and objects. Much easier to operate cocks term security than large-scale matrix fill unstructured access. Therefore, we may suggest a complex (critical) in the development of IS security policy to apply a combination of the two methods.

The second, equally important task is the development of CISS issues of protection from unauthorized access of IS, namely the implementation of identification and authentication of users. The identification of users by using methods that use some material an intimation (access key - "password" media key information - "smart card" measuring biometrics (eye's retina, fingerprints, speech recognition, etc.). These methods differ a complexity, reliability and cost of implementation. for complex (critical) IS appropriate to use methods based on measuring biometric characteristics of users as the most

reliable and accurate (because the unique parameters person do not change over time and are special) and promising technology in this area is to analyze the characteristics of Human DNA. Because users of IS exchange between a variety of documents, they should be sure that the documents are genuine. The authenticity of the documents provided by the use of electronic signatures, allowing through the use of cryptographic techniques (mathematical relationship between the document and the secret and public key digital signature) firmly establish the authorship and authenticity of the document. In this case, each user must have only one secret key and a list of public keys of users IS, formed a "security center" that is trusted by all users and which provides its control. The presence of the user private key, which is interconnected with the public key does not allow him to change his number in the IS and prevents him an opportunity to make signature to the number of another user.

In the third, some IS (including control systems, military systems) should take certain measures to protect against leakage through technical channels and counter reconnaissance equipment, in order to prevent information leaking confidential nature by hiding tell-tale signs, establishing active sources of influence on technical channels of information collection and so on.

III. CONCLUSIONS

Some aspects on the development of an integrated system of information security in the IS allow us to conclude that only through a comprehensive approach to the management and use of integrated software and hardware protection of information and appropriate organizational and technical measures possible target implementation of security policy in the IS. This material should be developers account when forming a comprehensive information security system in various information systems.

REFERENCES

[1] Московитов Н. Перспективы создания глобальной информационной сети МО США / Н. Московитов, Г. Рыбаков // Зарубежное военное обозрение. – 2013. – №7. – С. 8-19.

[2] Martovytskyi V.A. Модель мультиагентної системи збору та зберігання інформації / V.A. Martovytskyi, I.V. Ruban // Системи управління, навігації та зв'язку. Збірник наукових праць. – Полтава: ПНТУ, 2017. – Т. 6 (46). – С. 150-153

[3] Методология создания комплексной системы защиты информации/ Онацкий А.В. // Прикладная радио электроника: научн.-техн. журнал. — 2014. — Том 13. — № 3. — С. 350–356.

[4] [3] ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems —Requirements. [Електрон. ресурс]: – Режим доступу: http://www.itgivernance.co.uk/standards.arx

[5] [4] НД ТЗІ 3.7-003-05 "Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі". [Електрон. ресурс]: – Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article ?art_id=46074&cat_id=38835.

DOI: https://doi.org/10.30837/IVcsitic2020201367

Suricata intrusion detection and prevention system and its comparative analysis

Oleshko Inna[1]
[1]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine,inna.oleshko@nure.ua

Rykov Oleksandr[2]
[2]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine,oleksandr.rykov@nure.ua

Abstract. *The article is written about multitasking protecting program that helps users detecting intruders. It deals with application and shows how people can use this app to prevent stealing of their data. It was shown, that the Suricata program is one of the most popular and fast protector.*

Keywords: *administrator, traffic, network attack, Suricata, IDS, IPS, Snort.*

I. INTRODUCTION and Problem statement

Cyberattacks are one of the main problems faced by actors with information resources. Well-known antivirus programs and firewalls are only effective in protecting obvious access points to networks. However, attackers are able to find ways to bypass and vulnerable services even in the most advanced security systems. In today's world, Intrusion detection system / Intrusion prevention system (IDS / IPS) is a necessary element of protection against network attacks. The main task of these systems is to identify the facts of unauthorized access to the corporate network or unauthorized management of it, with the implementation of appropriate countermeasures (informing the administrators of the fact of intrusion, breaking the connection or re-configuring the firewall to block further actions of the attacker, etc.).

There are many intrusion detection and prevention systems. The urgent task is to choose one of them. The paper provides a comparative analysis of intrusion detection systems and concludes that Suricata is a faster and more reliable attack detector.

II. IDS / IPS- SYSTEMS

IDS / IPS systems are unique tools designed to protect networks from unauthorized access. They are hardware or software capable of promptly detecting and effectively preventing invasion. Measures taken to achieve the key IDS / IPS goals include informing security professionals about the facts of hacking and malware attacks, breaking off malicious connections, and re-configuring a firewall to block access to corporate data.

All intrusion detection and prevention systems that exist today are united by several common features, functions and tasks that can be solved by information security professionals. Such tools, in fact, perform continuous analysis of the exploitation of certain resources and identify any signs of atypical events.

Corporate network security can be based on several technologies that differ in the types of incidents detected and methods. In addition to the functions of continuous monitoring and analysis of what is happening, IDS systems perform the following functions:

- Collection and recording ofinformation;
- Alerts to network administrators of changes that have occured;
- Create reports for log summaries.

IPS systems can be considered as an extension of IDS, since the task of tracking attacks remains the same. In addition to the above, IPS technology can not only identify the threat and its source, but also block them. This speaks to the advanced functionality of such a solution. It is able to perform the following actions:

- Break off harmful sessions and prevent accessto critical resources;
- Change the configuration of the protection environment;
- Take action on attack tools (for example? Delete infected tools).

It is worth noting that the UTM firewall and any modern intrusion detection and prevention systems are the optimal combination of IDS and IPS technologies.

III. SURICATA ATTACK DETECTORS

Одним One of IPS's intrusion prevention solutions is attack detectors that are designed to detect a variety of malicious threats in a timely manner. In Internet Control Servers, they are implemented as a Suricata system, a multi-tasking and productive tool designed to protect networks, as well as collect and store information about any incoming signals. The work of the attack detector is based on the analysis of signatures and heuristics, and its convenience is due to the presence of open access to the source code. This approach allows you to customize the system performance for individual tasks.

The customizable Suricata settings include: rules that will be subject to traffic analysis, filters that limit the output of an admin alert, address ranges of different servers, active ports, and networks.

Thus, Suricata, as an IDS / IPS solution, is a fairly flexible tool that is subject to change depending on the nature of the attack, making it as effective as possible. Information and communication systems capture and store information about suspicious activity.

In the Suricata settings tab (Fig. 1) you can edit the settings of the attack detector. You can specify internal, external networks, address ranges of different servers, as well as the ports used. All of these variables are assigned a default value that the attack detector can correctly launch. By default, traffic to external interfaces is analyzed.

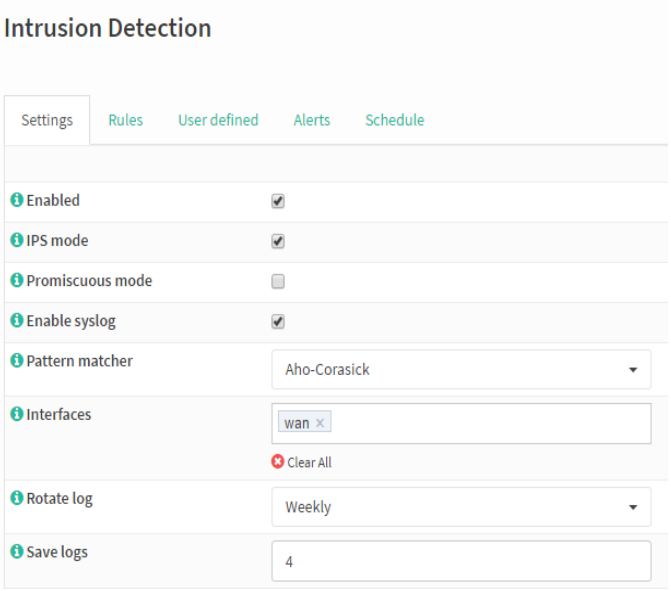


Figure 1. Suricata settings

Suricata Attack Detector can be connected to the rules by which it will analyze traffic. On the tab in Fig. 2, you can see the presence and contents of a rule file, and enable or disable its action (using the checkboxes to the right). In the upper right corner is a search by name or by the number of rules in the file.

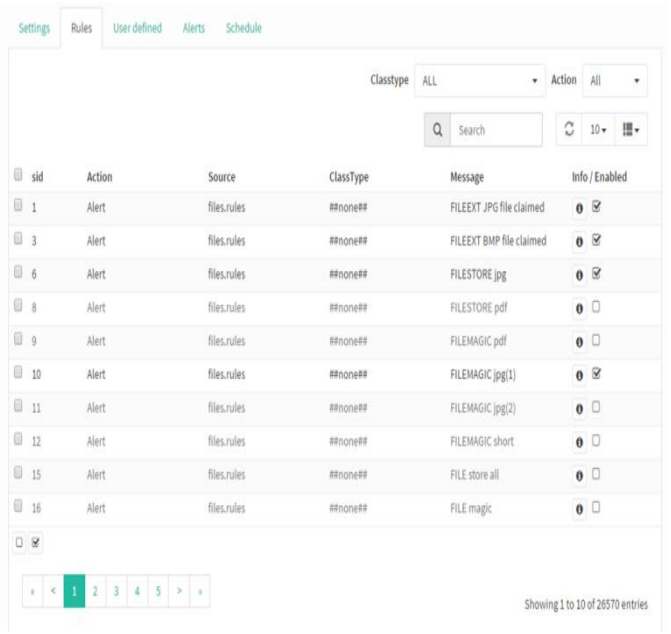


Figure 2. Suricata rules

IV. COMPARATIVE ANALYSIS SURICATA TA SNORT SYSTEMS

Snort is an IPS (Intrusion Prevention System) system for the network intrusion analysis. The software analyzes all traffic through the firewall searching for known attacks and anomalies. This program is free, open source GPL software and it is the most common IDS (and eventually IPS) in the world, thanks in large part to its openness and the work of authors.

More than 250 unit tests were conducted for Suricata and Snort systems. The test results are shown in Table 1.

The tests were conducted on 14 malware and viruses. As we can see from the table, Suricata has a better detection rate for malware and viruses than Snort.

On a set of 12 shells (virus hidden in another file), Suricata detected 12 shellcodes and Snort detected 7 shellcodes. In a set of 3 tests, both Suricata and Snort detected 3 DoS attacks against SSH and MSSQL. Tests have shown that Suricata is better than Snort for detecting client-side attacks. Out of 257 tests Suricata detected 157 attacks.

Table 1. Test results

Test group	Number of tests	Suricata score	Snort Score
Bad traffic	4	1	1
Broken packages	2	1	3
Malware	14	9	7
Denial of service (DoS)	3	3	3
Attacks from the client	257	157	127
Shells	12	12	7
Productivity	0	2	1
Total	297	185	149

V. CONCLUSIONS

Based on the above analysis, we conclude that Suricata Attack Detector is a fast and reliable system that maximizes the use of modern processors and GPUs. Tests have shown that Suricata is better than Snort for detecting client-side attacks and has better detection rate for malware and viruses than Snort. The disadvantage of Suricata can be considered a large number of settings and not enough detail in some issues documentation.

REFERENCES

[1] Anderson, James P., "Computer Security Threat Monitoring and Surveillance, " Washing, PA, James P. Anderson Co., 1980.

[2] Electronic resource https://oisf.net (date of appeal 20.10.2019)

[3] Electronic resource https://suricata-ids.org (date of appeal 20.10.2019)

[4] Electronic resource https://xserver.a-real.ru (date of appeal 25.02.2020)

[5] Electronic resource http://docs.nethserver.org(date of appeal 25.02.2020)

[6] Electronic resource https://cybrary.it (date of appeal 25.02.2020)

DOI: https://doi.org/10.30837/IVcsitic2020201368

Analysis of decentralized system identification schemes

Vlasov Andrii[1]
[1]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, andrii.vlasov@nure.ua*

Lysko Viktor[2]
[2]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine,* viktor.lysko@nure.ua

Abstract. *A scheme of identification system that uses the concept of building decentralized systems and allows each user to analyze the identity of users and service providers is considered. The main parameter of significance in the system is the level of trust in consumers depending on other participants of the platform and external information. It supports the ability for the owner to fully manage their data (account, master and secondary data) and its associated identifier through the use of various cryptographic signature mechanisms, hashing methods, and trust definitions implemented in decentralized systems and networks. The scheme is compatible with the digital asset management and current identification tools (for decentralized blockchain systems)*

Keywords: *digital identification, protocol, public key, hashing, consensus.*

I. Introduction and Problem statement

Global services, which have a large community of users worldwide, allow users to use different services through the OAuth protocol [1 - 5], which does not provide data reliability by cryptographic methods and uses session mechanisms to access user data.

The development of decentralized systems has shown that the best practice is the cryptographic signature of each request sent to the accounting system and the signature of each response that the system returns [5, 6].

A global digital identification system (decentralized systems and networks) should provide for the binding of all personal data (PD) of a user and his or her public key (key set) to a unique global identifier.

The purpose of building such a scheme is:

– all information about confirmation of personal data is stored in a single system. Using digital signature mechanisms and linking transaction sets to each other will allow the authentication of specific PD confirmations with event-bound events according to timeline [6].

– the integrity and authenticity of the data linked to the account is verified exclusively by cryptographic methods (the control root hash value of the Merkle tree) [7].

– the management of personal data is completely controlled by their owner, all other members of the system can only confirm the set that is defined by the user.

II. Problem solution and Results

In order to receive personally identifiable information about a particular member of the system, the identification service provider must contact the person directly and obtain or immediately require the required data set or permission to obtain this data from another provider.

A global user ID is unique within an identification system that represents a specific entity and related information. The ID is created by the public key of its owner, a set of hash values from his personal data, a set of hash values from the identifiers of other data of the accounting system.

All the above data are linked into one structure, which corresponds to both the account in the existing digital systems and the account (identifier) in the decentralized system (Table 1).

Table 1. Structure of the global user identification

Name	Mechanism of formation
Account (global) identifier	Generate a unique number when you create a new user account (size and range must be consistent with digital system protocol)
Public key	Generation by cryptographic signature methods (must match cryptographic protocol parameters, size and range - digital system protocol)
Readable identifier list	Calculation of hash values of different personal data of the user (must match the parameters of the selected hash methods, size and presentation - digital system protocol)
Main data confirmation list	Set of records (permanent information of personal data of the user), which are verified by a cryptographic signature (the minimum required data set for user identification, size and presentation must be consistent with the digital system protocol)
Merkle Root for main data	Calculation of hash values of the user's basic personal data set (must match the parameters of the selected hash methods, size and presentation - digital system protocol)
Additional data confirmation list	Additional set of records (variable information) of user data that is authenticated to them by a cryptographic signature (additional user data set, size and presentation must comply with digital system protocol)
Merkle Root for additional data	Calculation of the hash value of the additional set of personal data of the user (must match the parameters of the selected hash methods, size and presentation - digital system protocol)
Recovery power	Set of data (conditions) for restoring account access and changing the public key (the minimum required data set to restore access, size and presentation must match the parameters of the cryptographic protocol)
Providers list	Set of data from vendors implementing an authentication service

If the user chooses to restore some of the data for the full set, then the Merkle Root value will completely change. As a result, a previously created and sent transaction that confirms data for a particular Merkle Root becomes invalid. That is why the structure of the account has the peculiarity of splitting the data into main and additional parts: if the user has confirmed the basic data set (and does not change it), then regardless of whether the additional data have been updated, the master data remains confirmed.

A feature of decentralized systems is the lack of information in the network that directly determines the validity of a specific identifier: there are only accounts and voices that

confirm the data of the created accounts. Thus, the issue of trust is fully passed on to the client (he can personally determine the method by which his confidence level will be calculated).

Common methods of determining trust to date are:

– trust only to a specific (several) provider (the scheme is somewhat centralized if the number of providers the user trusts is small);

– trust by majority decision (number of IDs verified by network members). Being attacked by Sibyl - one of the accounts can create a large number of other accounts that confirm the identity of one of the members of the system);

– trust by most ISPs, vendors, and users (a more sophisticated validation algorithm that results in many levels of validation).

The main thing is that no matter how the consumer uses the results of the identification, the system provides the ability to fully customize the verification algorithm, which rests solely on the client's side.

Different algorithms (mechanisms) for reaching consensus are used to identify users' trust, determine their level of trust, and motivate validators in decentralized systems. In the blockchain systems, the Federated Byzantine Agreement and the Practical Byzantine Fault Tolerance are more expedient (rapid overall consensus on the network, advantage over participants' anonymity, and a higher level of decentralization) [7 - 9].

The key issue at this stage is protection against spam attacks: they cannot affect the decision-making mechanism of a specific ID, but this can negatively affect the system's bandwidth (since any user can add a transaction to the network, and in fact the number of such transactions is unlimited). Therefore, a mechanism should be provided for protection against this type of attack in the first place for validators.

The considered scheme of digital identification [7, 8] is capable of promptly responding to the compromise of user keys, since its states are homogeneous for all participants and all nodes at one point in time can receive information about the revocation of a separate certificate. It suggests using a secure method of recovering access to an account, which involves contacting multiple providers or other users (trusted by the user). The likelihood of collusion by all ISPs / other users (which support different authentication methods) is very low and allows the user to safely regain access to their account (although overall this complicates this procedure).

III. CONCLUSIONS

The blockchain digital identification scheme thus considered has the advantages over existing services:

complete control of users of their own data (change of account fields can be initiated only by their owners);

transfer of data management and decision-making to the end-user (independence of decision to make / reject individual identifiers);

making decisions by each party independently, focusing solely on the state of the database;

increased level of objectivity in verifying user data than using authentication from centralized providers;

the integrity and authenticity of the data linked to the account is verified solely by cryptographic methods;

the data set for the user implements multiple run of values with the calculation of their hash values;

repeated hashing of user data significantly increases the time needed for the attack from the attacker;

synchronization of events between independent parties through the use of blockchain technology (each party has the same state of the local database).

The use of blockchain technology to build different user identification schemes can solve the problem of providing an additional level of reliability and flexibility in the implementation of identification services (development of identification systems) in information and communication systems.

REFERENCES

[1] Using OAuth 2.0 to Access Google APIs. [online] Available at: https://developers.google.com/identity/protocols/OAuth2.

[2] Facebook Login for the Web with the JavaScript SDK. [online] Available at: https://developers.facebook.com/docs/facebook-login/web/.

[3] OAuth with the Twitter APIs. [online] Available at: https://developer.twitter.com/en/docs/basics/authentication/overview/oauth.

[4] Authorizing OAuth Apps. [online] Available at: https://developer.github.com/apps/building-oauth-apps/authorizing-oauth-apps/.

[5] RFC 6960: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – 2018. [online] Available at: https://tools.ietf.org/html/rfc6960.

[6] Distributed identities. [online] Available at: https://patents.google.com/patent/US7512649B2/.

[7] Oleksandr Kurbatov, Pavel Kravchenko, Nikolay Poluyanenko. "Global Digital Identity and Public Key Infrastructure." [ISCI'2019: Information security in critical infrastructures]. ASC Academic Publishing, Minden, Nevada, USA. pp. 237 – 247.

[8] Method, apparatus, and computer program product for providing a group based decentralized authorization mechanism [online] Available at: https://patents.google.com/patent/WO2009133419A1/.

[9] Protection of confidentiality, privacy and financial fairness in a blockchain based decentralized identity management system [[online] Available at: https://patents.google.com/patent/US20190182035A1/en?oq=US+20191820 35+(A1).

DOI: https://doi.org/10.30837/IVcsitic2020201369

The usage of dependency graphs to test the security of mobile software applications

Antonishyn Mykhailo

Pukhov Institute for Modelling in Energy Engineering, 15 General Naumov Str., Kyiv UA-03164, Ukraine, antonishin.mihail@gmail.com

Abstract. *Testing the security of mobile software applications by OWASP guidelines was analyzed. Attention is drawn to three levels of requirements in OWASP MASVS and their implementation under the OWASP MSTG guidelines. This guide identifies the processes and methods of testing mobile software applications for vulnerability. This leads to the arbitrary usage of these tools when verifying the feasibility of security requirements for mobile software applications. Overcoming the constraints is suggested by using dependency graphs, given the relationship between the testing stages.*

Keywords: *application security, mobile application security testing, MASVS, MSTG, OWASP, dependency graph.*

I. Introduction and Problem statement

Software applications for the Android operating system are increasing in popularity year by year. Therefore, one of the important aspects of their usage is safety. The security of mobile software applications is analysed by testing for vulnerabilities. For this purpose it is recommended to use the guidelines of OWASP MASVS and OWASP MSTG [1-3].

The requirements for the security of mobile software applications are set out in OWASP MASVS [3]. It defines two levels of requirements (MASVS-L1, MASVS-L2) and sustainability requirements (MASVS-R). The first level sets the general requirements for mobile software applications (MASVS-L1). Whereas the second one deals with the processing of highly sensitive data (MASVS-L2). The MASVS-R level reflects the requirements of preventing the implementation of threats by the user [1, 3, 4]. The feasibility of these requirements is analyzed according to the guidelines of OWASP MSTG [2]. This guide defines the processes and methods of testing mobile software applications for vulnerabilities [1, 2, 4].

However, when testing mobile application security on OWASP guidelines, it is up to the specialist to choose the right steps and tools. This leads, on the one hand, to the arbitrary choice of a sequence of steps and means of verifying the feasibility of security requirements. Whereas, on the other hand, it is difficult to reproduce the obtained results.

II. Problem solution and Results

To overcome these limitations, it is suggested to use dependency graphs [5]. The dependency graph is an oriented graph that displays the ratio of the multiple stages of mobile app security testing according to the selected transitive relationship (for example, the "pre-stage") over it:

$$G = (V, T), \qquad (1)$$

where V – is the set of stages of mobile app security testing according to OWASP guidelines, $V = \{v_i\}$, $i = \overline{1,n}$; T – is a transitive closure R on the set V, $T \subseteq R$; R – is a binary relation on the set V, $R \subset V \times V$.

Then, for example, testing a mobile application server with a static analyzer we get the following usage (1):

v_1 – running on a virtual machine;

v_2 – checking the ability to run on rooted devices;

v_3 – checking the possibility of debugging;

v_4 – checking for obfuscation and protection against tempering;

$$V = \{v_i\},\ i = \overline{1,4},$$
$$R = \{(v_1; v_2),\ (v_2; v_3), (v_3; v_4)\},\ R \subset V \times V,$$
$$v_1 R v_2 \Rightarrow v_2 R v_3 \Rightarrow v_3 R v_4,$$
$$v_1 T v_4.$$

III. Conclusions

Therefore, the feasibility of mobile application security is tested by OWASP guidelines. The choice of stages, means and sequence of their implementation is the responsibility of the specialist. This makes it difficult to reproduce the results. To prevent this, it is suggested to use dependency graphs in view of the relationship between testing stages.

References

[1] M. Antonishyn, and O. Misnik, "Analysis of testing approaches to Android mobile application vulnerabilities", Selected Papers of the XIX International Scientific and Practical Conference "Information Technologies and Security", Ukraine, vol. 2577, pp. 270-280, November 2019. [Online]. Available: http://ceur-ws.org/Vol-2577/paper22.pdf.

[2] OWASP Mobile security testing guide (MSTG). [Online]. Available: https://github.com/OWASP/owasp-mstg/.

[3] OWASP Mobile application security verification standard (MASVS). [Online]. Available: https://github.com/OWASP/owasp-masvs.

[4] M. Antonishyn, "Android application security assessment," UP2IT conference. [Online]. Available: https://www.slideshare.net/Mykhailo Antonishyn/android-pentesting-189736097.

[5] J. Gross, J. Yellen, and M. Anderson, Graph Theory and Its Applications. Boca Raton, USA: CRC Press, 2019.

DOI: https://doi.org/10.30837/IVcsitic2020201370

Conceptualization of knowledge about information security management system

Mokhor Volodymyr[1]

[1]Pukhov Institute for Modelling in Energy Engineering of National Academy of Sciences of Ukraine, 15 General Naumov Str., Kyiv UA-03164, Ukraine, v.mokhor@gmail.com

Tsurkan Vasyl[2]

[2]Pukhov Institute for Modelling in Energy Engineering of National Academy of Sciences of Ukraine, 15 General Naumov Str., Kyiv UA-03164, Ukraine, v.v.tsurkan@gmai.com

Dorohyi Yaroslav[3]

[3]National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", 37 Prosp. Peremohy, Kyiv UA-03056, Ukraine, argusyk@gmail.com

Shtyfurak Yurii[4]

[4]National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", 37 Prosp. Peremohy, Kyiv UA-03056, Ukraine, yura.shtyfurak@gmail.com

Abstract. *The use of ISO / IEC 27000 and ISO Guide 73 standards as glossaries of terms regarding the information security management system is considered. The establishment of correlation between terms on the ontological approach is shown. Attention is drawn to its applicability to the presentation of organizational guidelines and deadlines for risk. Against this background, conceptualized knowledge about the ontology information security management system, taking into account the systematic approach. This system is presented as a complete entity with stable structural and functional links between its elements.*

Keywords: *information, risk, information security, information security management systems, conceptualization, ontology.*

I. Introduction and Problem statement

Information security management systems are developed using the terms and definitions of ISO / IEC 27000 [1]. At the same time, this glossary is supplemented by terms on risk and risk management in general [2]. Both documents are focused on creating a unified approach to defining and interpreting the concepts of information security management system [1, 2].

The relationships between the terms based on the ISO / IEC 27k series are determined ontologically. Its use makes it possible to establish relationships between security concepts and standards, in particular, ISO / IEC 27001. A characteristic feature of such relationships is the orientation either to the attainment of organizational guidelines or to terms regarding risk (asset, vulnerability, threat, risk). Recommendations for the practical application of such ontologies are given in [3, 4].

II. Problem solution and Results

Knowledge about the information security management system is conceptualized in a systematic approach. It is regarded as a coherent entity consisting of a set of structurally and functionally interrelated elements. The integrity of the object is ensured by a set of strong links between the elements that make up the structure of the information security management system.

The ontology of an information security management system is defined by an interconnected and coherent set of three components [5, 6].

$$O = \langle X, \Re, \Phi \rangle, \quad (1)$$

where O – ontology; X – non-empty finite set of terms regarding the information security management system; $\Re$ – finite set of relations between terms; Φ – finite set of interpreting functions defined in terms and/or relationships of an ontology.

If $\Re = \varnothing$ and $\Phi = \varnothing$, then (1) displays a glossary V of terms according to ISO/IEC 27000, ISO Guide 73 [1, 2, 5, 6]

$$O = \langle X, \{\}, \{\} \rangle,$$

$$O = V.$$

III. Conclusions

Therefore, knowledge about the information security management system is conceptualized using an ontology with a systematic approach. For this purpose, the dictionaries of ISO/IEC 27000, ISO Guide 73 and, secondly, the presentation of the system as a whole entity with a set of structurally and functionally interrelated elements were used.

References

[1] International Organization for Standardization. (2018, Febr. 7). ISO/IEC 27000, Information technology. Security techniques. Information security management systems. Overview and vocabulary. Geneva. [Online]. Available: https://www.iso.org/ru/standard/73906.html.

[2] International Organization for Standardization. (2016, Jan. 21). ISO Guide 73, Risk management, Vocabulary. Geneva. [Online]. Available: https://www.iso.org/standard/44651.html.

[3] I. Meriah, and L. B. Arfa Rabai, "Comparative Study of Ontologies Based ISO 27000 Series Security Standards", Procedia Computer Science, vol. 160, pp. 85–92, 2019, doi: 10.1016/j.procs.2019.09.447.

[4] P. Sirisom, J. Payakpate, and W. Wongthai, "A System Design for the Measurement and Evaluation of the Communications Security Domain in ISO 27001:2013 Using an Ontology", in Information Science and Applications, vol 424, K. Kim, and N. Joukov, Eds. Singapore: Springer, 2017, pp. 257–265, doi: 10.1007/978-981-10-4154-930.

[5] M. Uschold, and M. Gruninger, "Ontologies principles methods and applications", Knowl. Eng. Rev, vol. 11, no. 2, pp. 93–155, 1996.

[6] T. A. Gavrilova, and V. F. Khoroshevskii, Intelligent systems knowledge base, Kharkiv: Piter, 2000.

DOI: https://doi.org/10.30837/IVcsitic2020201371

Presentation the interaction of the subject and the object of socio-engineering influence with a social graph

Tsurkan Oksana[1]
[1]*Pukhov Institute for Modelling in Energy Engineering, 15 General Naumov Str., Kyiv UA-03164, Ukraine, otsurkan24@gmail.com*

Herasymov Rostyslav[2]
[2]*Pukhov Institute for Modelling in Energy Engineering, 15 General Naumov Str., Kyiv UA-03164, Ukraine, gerasimov.rostislav@gmail.com*

Kruk Olha[3]
[3]*Pukhov Institute for Modelling in Energy Engineering, 15 General Naumov Str., Kyiv UA-03164, Ukraine, o.n.kruk@gmail.com*

Abstract. *The use of social engineering as an interaction between an attacker and an employee is considered. It shows its focus on receiving sensitive information. This is achieved by an attacker by studying, engaging, trusting, using employee trust. To prevent this, psycho-personal qualities, professional competences of the social engineer and employee are taken into account, and their interaction is represented by a social graph. Its tops reflect a social engineer, employee, quality and compensation; connections – the relationship between them. This approach will make it impossible to manipulate the employee's mind.*

Keywords: *social engineering, social interaction, manipulation, forms of manipulation, social graph.*

I. Introduction and Problem statement

The use of social engineering is reduced to the interaction of the attacker with an employee of the organization. Such interaction is focused on receiving confidential information and is implemented in four phases: studying, establishing interaction, entering into trust, using trust [1-3].

An example of the study of these phases is the social engineering optimizer. They are used by separating the attacker (social engineer) and protector (employee of the organization). Each is initialized by two random decisions. Better among them is interpreted as an attacker. To achieve this, he adheres to social engineering methods [4].

However, the consideration remains that during the interaction, the social engineer manipulates the employee's consciousness and, as a consequence, gains sensitive information.

II. Problem solution and Results

According to the socio-engineering approach the vulnerabilities of the employee are interpreted as his weaknesses, needs, mania (passions), admiration. This leads to a new model of his behavior, creating favorable conditions for the implementation of threats to the use of social engineering. The manifestation of such forms is fraud, deception, scam, intrigue, hoax, provocation. The social engineer intentionally influences the employee's mind against will, but with his or her consent.

Therefore, it is important to take into account their psychological and personal qualities and professional competences when interacting.

In order to take into account the psychological and personal qualities, professional competencies of the social engineer and the employee of the organization, it is recommended that their interaction be represented by a social graph [5, 6].

Social graph represents the interaction of the subject (social engineer) with the object (employee of the organization) of socio-engineering influence and the connection between them

$$G = (V, E),$$

where G – social graph; V – set of peaks (e.g., social engineer, employee, software tool, psychological and personal qualities, professional competences); E – set of connections (e.g., "social engineer – employee", "social engineer – software tool", "employee – software tool", "employee – qualities").

III. Conclusions

Thus, the use of social engineering is reduced to manipulating the attacker with the employee's mind against the will, but with his or her consent. To prevent this, the psycho-personal qualities, professional competencies of the subject and the object of such interaction are taken into account by presenting them with a social graph.

References

[1] O. Tsurkan, R. Herasymov, and O. Kruk, "Methods of counteracting social engineering", Information Technology and Security, vol. 7., iss. 2 (13), pp. 161-170, July-December 2019, doi: 10.20535/2411-1031.2019.7.2.190563.

[2] F. Mouton, L. Leenen, and H. Venter, "Social engineering attack examples, templates and scenarios", Computers & Security, vol. 59, pp. 186-209, September 2016, doi: 10.1016/j.cose.2016.03.004.

[3] S. Ellis, "Social Engineering Deceptions and Defenses", in Computer and Information Security Handbook, J. Vassa, Eds. Burlington, USA: Morgan Kaufmann, 2017, pp. 465-474, doi: 10.1016/B978-0-12-803843-7.00029-6.

[4] A. Fathollahi-Fard, M. Hajiaghaei-Keshteli, and R. Tavakkoli-Moghaddam, "The Social Engineering Optimizer (SEO)", Engineering applications of artificial intelligence, vol. 72, pp. 267-293, June 2018, doi:10.1016/j.engappai.2018.04.009.

[5] V.V. Mokhor, O.V. Tsurkan, R.P. Herasymov, and V.V. Tsurkan, "Information Security Assessment of Computer Systems by Socio-engineering Approach", Selected Papers of the XVII International Scientific and Practical Conference "Information Technologies and Security". Kyiv, 2017. pp. 92-98. [Online]. Available: http://ceur-ws.org/Vol2067/paper13.pdf.

[6] J. Gross, J. Yellen, and M. Anderson, Graph theory and its applications. Boca Raton, USA: CRC Press, 2019.

FLEXIBLE INTEGRATED SYSTEMS AND ROBOTICS

DOI: https://doi.org/10.30837/IVcsitic2020201372

Basic Classes Of Mathematical Models Used In Machine Vision Problems

Yeromina Nataliia[1]
Lukashyn Oleksii[2]

[1]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, nataliia.yeromina@nure.ua
[2]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, oleksii.lukashin@nure.ua

Abstract. *Today, computing platforms are a booming industry. However, a huge gap in the technology of "artificial intelligence" and its important component parts – understanding scenes and images – is, in fact, a major limiting factor for further development of complex control systems. In this article we consider the basic classes of mathematical models used in the development of practical image analysis systems currently.*

Keywords: *machine vision, **i**mage analysis, simulation modeling, abstract modeling, mathematical model.*

I. Introduction and Problem statement

Machine vision is a scientific field in the field of artificial intelligence and robotics, as well as related technologies for obtaining images of real-world objects, their processing and use of the obtained data to solve various kinds of applied problems without human intervention.

In various technical problems in the field of machine vision chosen certain basic ways of describing reality. Let's see in which cases it is better to use some methods, and in which others. There is no single universal solution here, but at the most general level, as two "extreme" poles, two basic fundamentally different approaches can be mentioned here: simulation (physical) modeling and abstract (brightness-geometric) modeling[1].

Simulation in the field of machine vision involves an attempt to describe some real physical object and a real physical device for acquiring an image of this object. The advantage of this approach is the completeness and reliability of the simulation results, as well as the guaranteed quality of image analysis methods based on simulation models. The disadvantages of the simulation approach are associated with a disproportionate amount of labor at the stage of compiling the model and too much experimental data needed to build the simulation model.

Abstract modeling proceeds from the most general considerations about the nature of the analyzed objects and the way they are registered. Such an approach in the literature is sometimes called iconic [2]. The advantages of the iconic approach are that when developing image analysis methods, a minimum of a priori information about a real observation situation is required. The main drawback of abstract modeling is determined by the high probability that a method developed for a too general model will turn out to be either generally inoperative or substantially less effective in practice than methods created based on models that are specific to this task.

In practice, both approaches are rarely found in their pure form. Often, developers start from general abstract models, which are then gradually concretized and adapted to the available real data, thereby approaching simulation models. At the same time, it must be considered that the same methods and models, depending on the field of application, can pass from the class of simulation models to the class of abstract ones, and vice versa [3].

II. Problem solution and Results

Consider the basic classes of mathematical models used in image analysis, their differences and peculiarities.

Image as a function of vector argument

Often, the initial description of an image in practice is a two-dimensional intensity function.

Many methods of image analysis, in which images are considered as two-dimensional functions, suggest that the concepts of addition and multiplication of functions, multiplication of a function by a number, scalar product of functions, norm of a function, linear space, etc. are defined. All these concepts can be transferred to the domain image analysis all known methods and results from the field of linear algebra and vector spaces [2].

It is also often assumed that function images are the required number of times continuously integrable and differentiable. This allows you to transfer to the field of image analysis all known methods and results from the field of functional analysis [4].

Representation of the image in the form of a set of points

Representation of the image in the form of a set of points makes it possible to determine the operations of union, intersection, addition, and the inclusion relation for images, thereby extending to the field of image analysis methods and results from the field of set theory [5].

Image as a topological object

An image presented as a collection of points (point pattern) can be considered as a topological object, i.e. described in terms of topological elements: connected areas, boundaries of areas, connected lines and isolated points. Accordingly, topological similarity measures and topological transformations can be defined that preserve or change in a certain way the topological properties (number and ratio of topological elements) of an image. Thus, presenting an image in the form of a list or a set of points also allows you to transfer methods and results from the field of topology to the field of image analysis. In particular, the theory of coatings, being transferred to the field of analysis of discrete binary and then grayscale images (regarded as "shadows"), led to the creation of Serre's mathematical morphology [6].

If, in addition, we are dealing with metric space, then all methods of cluster analysis are automatically applied to lists of image points [7].

Image as a geometric object

After topology and metric were introduced on the sets of points, the next step was to consider images as geometric objects.

From the field of analytic geometry, image analysis borrows the following basic elements:

- geometric transformations of images, properties of these transformations;
- parametric description of the sets of points in the coordinate space;
- "Geometric logic" (reduction from planimetry and stereometry, rules of geometric inference);
- ways to build and find figures.

Analysis of images based on models can be considered as a kind of "generalized geometry", the differences of which from classical geometry are as follows.

- Bright-geometric aspects. Here the difference compared to the classical geometry are continuous in the transition from points, lines and surfaces to discrete lines, areas and volumes; shifting the focus of attention from simple and "right" figures to complex nonanalytic forms; the presence of the considered geometric objects of additional non-geometric characteristics (intensity, color, etc.).
- Logical-probabilistic aspects. Classical geometry never considers false, interfering, or inaccurate data. In this regard, the classical problem of substantiating the conclusions and decisions obtained also receives a broader interpretation in the analysis of images. The rationale for the decision can be strictly logical, but more often it is probabilistic or fuzzy.
- Computational aspects. The specifics of modern image analysis tasks are determined by the need to consider the specific architecture, memory size and performance of a given computer under the indicated restrictions on these parameters.

Image as a set of independent features

The image as a set of independent features represents the completion of the idea of representing the image as a set of independent informative elements. In this case, there is a transition from an arbitrary set of informative elements (geometric points, information vectors) to a more rigid structure – an ordered set of informative elements of a given size, that is, to a feature vector.

Image as a structure

Structural models of images make it possible to transfer to the field of image analysis all known methods and results from the field of structure analysis, which, however, itself was created under the significant influence of problems from the field of geometry and image analysis. In general terms, the definition of a structural model can be represented as: "a set of elements of given types that satisfy a set of conditions that describe the relationships of given types" [3].

Image as a two-dimensional projection of a three-dimensional scene.

The photogrammetric approach [8], which considers individual images and ensembles of images as two-dimensional projections of three-dimensional scenes recorded using optical systems of a specific configuration (distances and angles between cameras, passport data and distortions of camera lenses), of course, is an essential step towards simulation.

However, this approach is still not based on physical, but on geometric modeling, since it is traditionally limited by considering the geometry of the survey and does not imply an analysis of other physical factors affecting the quality of the resulting image.

The mathematical apparatus used in photogrammetry is entirely based on stereometry, projective geometry, and geometric optics.

Further, this approach can be developed by combining it with a structural approach. The task of stereo reconstruction, as well as the task of detecting and identifying objects, is thus reduced to the problem of optimal indexing of a three-dimensional structural graph in an image or ensemble of stereo images [3].

Used in the modern literature on machine vision, the term high-level model approach involves solving this problem of identifying (linking) a three-dimensional structural model of an object.

III. CONCLUSIONS

The analysis of the subject area showed that although for each individual task of analyzing images one or the other classes of mathematical models show themselves better than the others, but for the task of localizing the binding objects of a system of mobile robots, the most universal from the point of view of flexibility and ease of use is the representation of the image in the form of a set points. flexibility and ease of use, we highlight the fundamental criteria when choosing a target mathematical model.

REFERENCES

[1] Ruban, I., Smelyakov, K., Vitalii, M., Dmitry, P., & Bolohova, N. (2018, May). Method of neural network recognition of ground-based air objects. In *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)* (pp. 589-592). IEEE.

[2] Yaroslavsky L.P. Digital Signal Processing in Optics and Holography: An Introduction to Digital Optics. - M.: Radio and communication, 1987.

[3] Yu.V. Wieselter, S.Yu. Zheltov, A.V. Bondarenko, M.V. Ososkov, A.V. Walrus. Image processing and analysis in machine vision tasks: Course of lectures and practical classes. - M.: Fizmatknig, 2010. - 672 pp.

[4] Lefort G. Algebra and Analysis. - M.: Science, 1973.

[5] Kuratovsky K., Mostovsky A. Set theory. - M.: Mir, 1970.

[6] Serra J. Image Analysis, Mathematical Morphology. – Academic Press, 1982.

[7] R. Duda, P. Hart, Pattern Classification and Scene Analysis. – New York: John Wiley & Sons, 1973.

[8] Lobanov A.N. Photogrammetry. - M.: Nedra, 1984.

DOI: https://doi.org/10.30837/IVcsitic2020201373

Situation Representation Model Implemented by Granule Fuzzy Characteristics in Mobile Autonomous System

Kargin Anatolii[1]
[1]Ukrainian State University of Railway Transport, Feyerbakh square, 7, Kharkov, 61050, kargin@kart.edu.ua

Luchentsov Yevhen[2]
[2]Ukrainian State University of Railway Transport, Feyerbakh square, 7, Kharkov, 61050, luchentsov@kart.edu.ua

Abstract. *Creation of the mobile autonomous control system has specifics. The decision-making and assessment of the large scale situation are based on the global situation model presented in the form of a multilevel structure at different abstraction levels. Three types of abstraction are considered: quantitative, deterministic, and generalized abstraction. The report examines the algorithm for processing data from sensors at the first two levels. Algorithm is programmed in Python and implemented on ESP 8266 microcontroller.*

Keywords: *mobile autonomous systems, global situation model, quantitative and determinative abstraction, granule fuzzy characteristics.*

I. Introduction and Problem statement

Large scale situation assessment systems, organized on a distributed monitoring basis, include local components that move across the monitoring object space and are implemented as mobile autonomous systems (MAS). The decision-making and assessment of the situation in these systems are based on the global situation model (GSM) [1], which is based on data obtained from MAS. In work [2], GSM is proposed in the form of a multilevel structure at different levels, the situation of which is represented by concepts of different levels of abstraction. Model [3] formalized three types of data abstraction: quantitative, deterministic, and generalized abstraction. Quantitative and determinative abstraction (Q&DA) acts as a bridge between natural language description and numerical sensor data. The report examines the first two levels of abstraction of Q&DA for the representation of GSM in MAS.

At the department of Information Technologies of USURT, the applications creation technologies, including MAS, are tested on the basis of a training and research polygon of the Internet of Things and Intelligent Machines [1]. In the report, a wheeled robot performing the function of monitoring the occurrence of a fire situation is views as a MAC. The robot is implemented on a four-wheeled chassis with gear motors, equipped with a single-board Raspberri Pi 3B computer, Arduino Motor Shield controller and ESP 8266 microcontroller. Data acquisition from DHT11 temperature and humidity sensors, BH1750 smoke, MQ - 2 flame and illumination and Q&DA is implemented on ESP 8266 microcontroller. The report examines the algorithm for processing data from sensors at the first two levels of Q&DA. Algorithm is programmed in Python and implemented on ESP 8266 microcontroller.

II. Problem solution and Results

The algorithm uses knowledge of granulation of a control variable: how many granules are by the range of possible variable values) and fuzzy restrictions for these granules. The fuzzy characteristic of the pellets is the fuzzy confidence factor [2, 3]. Therefore, the fuzzy constraints of the granules are set as a function of the fuzzy confidence factor given in the variable definition area, as shown in Fig. 1.

Q&DA is a procedure of granulating data from each source and determining granules fuzzy characteristics (GFC) [3]. For this, set of possible sensor values covered by several information pellets. The size and number of granules depends on the task. Each of these granules refers to the zero level of GSM. The fuzzy characteristic of the pellets is a fuzzy L-R number with a Gaussian function with three parameters: α - confidence; TL and TR are the time intervals since the last sensor data was received and the data changed, respectively. On the basis of GFC there is an integral characteristic of confidence - a confidence factor CF [3].

The universal model for presenting knowledge about granulating data from a single sensor is as follows:

$$<n, (a_1, b_1, c_1, d_1, e_1, f_1), \ldots, (a_i, b_i, c_i, d_1, e_i, f_i), \ldots, (a_n, b_n, c_n, d_n, e_n, f_n)>, \quad (1)$$

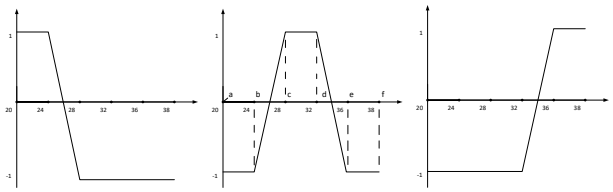
where n – is the number of granules into which the area of possible data from sensor is broken;

$a_i, b_i, c_i, d_1, e_i, f_i$ – are parameters of a piecewise linear function representing the distribution of confidence α over the range of possible data from sensor.

The meaning of the parameters $a_i, b_i, c_i, d_1, e_i, f_i$ explains Fig. 1b. Consider an example where the data from the temperature sensor is represented by 3 granules. Formula (1) for this case will be:

$$<3, (a_1 = 20, b_1 = 20, c_1 = 20, d_1 = 24, e_1 = 28, f_1 = 38), (a_2 = 20, b_2 = 24, c_2 = 28, d_2 = 32, e_2 = 36, f_2 = 38), (a_3 = 20, b_3 = 32, c_3 = 36, d_3 = 38, e_3 = 38, f_3 = 38)> \quad (2)$$

The numerical definition of the three granules in (2) is shown graphically in Fig. 1 and corresponds: the first granule is shown in Fig. 1a, the second is shown in Fig. 1b, and the third is shown in Fig. 1.c.



a) b) c)

Figure 1. Graphical view of the numerical definition

In accordance with the abstraction model [2,3], an algorithm for granulating the input numerical values and extracting GFC in real time was developed. The granulation algorithm for a single data processing step on the example of a single temperature sensor is shown below.

1. Obtaining data from the temperature sensor T.
2. Validation of data $T \in [T_{min}, T_{\max}]$.
3. Calculation of the confidence parameter α.

$$\alpha = \begin{cases} -1 & \text{if } T \in (a,b],\ b \neq T_{\min} \text{ or } T \in (e,f]; \\ -1 + 2\dfrac{T-b}{c-b} & \text{if } T \in (b,c],\ c \neq T_{\min}; \\ +1 - 2\dfrac{T-d}{e-d} & \text{if } T \in (d,e]; \\ +1 & \text{if } T \in (c,d]. \end{cases} \quad (3)$$

4. Calculation of confidence parameters t_L and t_R

$$t_L = 0, \quad (4)$$

$$t_R = \begin{cases} 0, & \text{if } (\alpha \geq \varepsilon \ \ \& \ \ \bar{}q = 0) \text{ or } (\alpha \leq -\varepsilon \ \ \& \ \ \bar{}q = 1); \\ \bar{}t_R + 1, & \text{therwise}, \end{cases} \quad (5)$$

III. CONCLUSION

The following example demonstrates the efficiency of a program. The results of a survey of the temperature sensor at the current step gave T = 27º. Assuming that in the previous step were the values of $GFC_1 = (\alpha_1 = -1.0, t_{L1} = 0, t_{R1} = 10)$, $GFC_2 = (\alpha_2 = -1.0, t_{L2} = 0, t_{R2} = 10)$, $GFC_3 = (\alpha_3 = 0.75, t_{L3} = 0, t_{R3} = 10)$ and $\varepsilon = 0.75$. Calculations according to the above algorithm based on knowledge (2) gave the following values of the parameters of GFC for these granules: $GFC_1 = (\alpha_1 = -0,5, t_{L1} = 0, t_{R1} = 11)$, $GFC_2 = (\alpha_2 = 0.5, t_{L2} = 0, t_{R2} = 11)$, $GFC_3 = (\alpha_3 = -1, t_{L3} = 0, t_{R3} = 0)$.

REFERENCES

[1] A. Kargin,. O. Ivaniuk, G. Galych, A. Panchenko, “Pollygon for smart machine application“, 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies DESSERT’2018, Ukraine, Kyiv, May 24-27, 2018, P. 489-494.

[2] A. Kargin, T. Petrenko, “Abstraction and categorization in smart machines based on granular computations.” Vestnik Natsional'nogo tekhnicheskogo universiteta" KhPI". Seriya: Informatika i modelirovaniye, vol. 50(1271), pp. 57-68, 2017. (in Russian)

[3] A. Kargin, T. Petrenko, “Internet of Things Smart Rules Engine”, in 2018 Inter. Sci.-Pract. Conf. Probl. Infocommun. Sci. and Technol. (PIC S&T 2018), Kharkiv, Ukraine, Oct. 9-12, 2018, pp. 639-644.

DOI: https://doi.org/10.30837/IVcsitic2020201374

Intelligent manipulation control for robotic system

Tsymbal Oleksandr[1]
[1]Kharkiv National University of Radio Electronics, Nauki Ave. 14, Kharkiv, 61166, Ukraine, oleksandr.tsymbal@nure.ua

Mordyk Oleksandr[2]
[2]Kharkiv National University of Radio Electronics, Nauki Ave. 14, Kharkiv, 61166, Ukraine, kurtwalkir@gmail.com

Abstract. *There is provided an analysis in development of flexible integrated systems of industrial application. Report shows an increasing importance of intelligent components for control systems. There are considered the basic items on development of intelligent decision-making support systems to solve the manipulation tasks of industrial robots. The language-oriented constructions for knowledge bases of intelligent problem solvers are presented as well as specifications of their practical implementation and perspective development directions.*

Keywords: *intelligent control; decision-making support; intelligent problem solver; robotics; manipulations.*

I. INTRODUCTION

The analysis of tendencies of development of flexible integrated production systems indicates the increasing complexity of the organization of modern production, both at a separate workplace and in the conditions of a workstation, workshop or plant. In these circumstances, the role of automated control systems that use AI tools capable to obtain, with good quality, information about the state of production systems, to analyze them, and to make decisions to ensure the functioning of the enterprise, is growing. The role of production decisions in every specific workplace, which becomes a function of servicing equipment: industrial robots, robocars, other providing and technological systems [1, 2], is increasing. At the same time, the problem of the development and implementation of intellectual support for decision-making at different levels of management of flexible integrated production systems remains actual.

II. BASIC TASKS OF INTELLIGENT CONTROL SYSTEMS FOR MANIPULATIONS

The plan of decision for manipulation robot is described as a sequence of actions, starting from the beginning, through the transformation of the states of the system – to the achievement of the goal (or goals). Among the implementations of planning systems there should be mentioned such systems as STRIPS, NONLIN, PRODIGY [2]. The planning process is divided into decomposition and coordination phases [3].

The plan development system consists of a general problem solver associated with many training modules; the system also includes the following components: EBL (Explanation-based learning), blocks for defining analogy derivatives, abstraction of plans, and validation. The descriptive language implemented, for example, in PRODIGY (PDL) is a form of predicate logic that supports standard logic operations for multiple sets of elements [4].

In order to describe the plan generator as a tool to process rules and to implement the planning process, and in order to solve concurrently existing tasks (two-handed implementation), [2] proposes language CSA. Here, the rules are described using CSA formulas. The CSA plan generator manipulates pre- and post-conditions. To describe the rules for workspace with three blocks, the pre- and post-conditions C1 - C4 are defined as:

$$C1 = ONTABLE(x) \wedge CLEAR(x) \wedge HANDEMPTY$$
$$C2 = HOLDING(x)$$
$$C3 = HOLDING(x) \wedge CLEAR(y)$$
$$C4 = HANDEMPTY \wedge CLEAR(x) \wedge ON(x, y)$$

To define all the possible conditions, there are used operators to update the conditions and identity statements for description. The status of the current situation is described by rules such as PICKUP, PUTDOWN, STACK, UNSTACK. The identity statement indicates the conditions for non-compliance. The problem solver consists of working memory, knowledge base (rules, frames, networks) and inference engine [5].

The inference engine creates function of possible actions to the current state, generates new routs. The planning process includes stages of description of current system's state; of search of rules (by inference engine) corresponding to currents state; of finding rules, corresponding to current state for inference engine; of creation (by inference engine) transitions for current state and generation of new system's states.

The further use of strategic planning methods should be based on logical models, considering the dynamic nature of intellectual robotic manipulation systems.

III. CONCLUSION

The current problem with modern flexible integrated production systems still remains in a the provision of production functions under the effect of various external factors, including those associated with changes in the conditions of execution of technological operations, adaptation to new conditions of production technology, interaction with other technological equipment. These tasks can be solved by the decision support systems of intelligent control systems, implemented for mobile and manipulation robots.

REFERENCES

[1] O. Tsymbal, A. Bronnikov, A. Yerokhin. Adaptive Decision-making for Robotic tasks // Proceeding of IEEE 8th Conf. Advanced Optoelectronics and Lasers, CAOL-DSMOLE*2019: "Data Science in Modern Optoelectronics and Laser Engineering", Sept. 6-8, Sozopol, Bulgaria. – P. 594-597.

[2] Xin-She Yang (ed). Artificial Intelligence, Evolutionary Computing and Metaheuristics. Springer, 2013, 796 p.

[3] Zheng C., Liu H., Ge M., Liu Y. A Novel Maze Representation Approach for Finding Filled Path of a Mobile Robot, Int. Conf. Computer, Network, Communication and Information Systems (CNCI 2019), Advances in Computer Science Research, volume 88, pp. 664-673, 2019.

[4] Tsymbal O., Bronnikov A. Decision-making information technology for flexible integrated manufacturing / Modern state of science researches and technologies. 2019. № 2 (8). – C. 105-112.

[5] Bronnikov, I. Nevliudov, O. Tsymbal. Flexible manufacturing tendencies and improvements with visual sensoring / Eskisehir Technical University Journal of Science and Technology. Applied Sciences and Engineering, 2019. Vol. 20, ICONAT issue, P. 77-83.

DOI: https://doi.org/10.30837/IVcsitic2020201375

Integrated systems and robotics in forensics

Sezonova Iryna[1]

Sezonov Victor[2]

[1]*Kharkiv National University of Radio Electronics, Nauki Ave. 14, Kharkiv, 61166, Ukraine, iryna.sezonova@nure.ua*

[2]*Kharkiv Research and Forensic Center, Kovtuna st.32, Kharkiv, 61036, Ukraine, sv26031985@gmail.com*

Abstract. *The article reviews the problematic aspects of the development and improvement of forensic activities. The authors proves the necessity of forming a new separate branch of criminalistic technique. The authors proposes the new termin – "The Criminalistic robotechnology" – for it. Along with the effective use of existing tools and methods of application of special knowledge in the detection and investigation of crimes, also addresses the problem of developing new, based on modern technologies.*

Keywords: *innovative technologies; forensic examination; forensic activities; criminalistic robotechnology; criminalistic technique; robocop.*

I. INTRODUCTION

The latest achievements of scientific and technological progress have made it possible to improve the work of forensic experts so much that the solution of many tasks of forensic examination without the use of modern information technologies has become impossible. Currently, work is underway to create a collection of digital computer models of objects of technical and forensic research of documents. Automated workstations for forensic experts of various expert specialties (trasologist, ballista, economist, phonoscopist, psychologist, etc.), new devices and complexes of functional devices for research and recording of evidence, developed techniques for the study of new objects of forensic examination, created various information retrieval systems and databases. The possibilities of forensic biological research using modern advances in mathematical modeling have been greatly expanded. At present, in practice, robots are used that allow recognizing explosive devices, penetrate into small rooms with video surveillance function, and replace the non-malfunctioning process.

II. BASIC TASKS OF INTELLIGENT CONTROL SYSTEMS FOR MANIPULATIONS

The process of development of forensic expertise is directly dependent on the needs of investigative and judicial practice. It determines the relevance of various scientific studies necessary to establish circumstances relevant to the investigation of crimes. The level of knowledge in various fields of science and the development of general methods of cognition, on the one hand, and changes in the forms of criminal procedure, the role of forensic science in this process, and the norms governing its activities affect the development of forensic science and the degree to which innovative technologies are used in forensic research - with another.

In Ukraine, the Evrika forensic examination support system has been developed to conduct examination of cable products in the wake of reflows. Flexible systems and databases have been created - Dagger _ (cold steel examination), Baleks (forensic ballistic examination), Narcoex (for the study of narcotic substances), FARA (for the study of headlights of vehicles and their fragments) other. The use of innovative technologies allowed expanding the possibilities of technical and forensic research of documents, increasing the reliability and scientific level of research in solving most expert problems. For example, using metallographic microscopes with a 500-fold magnification, equipped with digital photo or video, it became possible to establish the sequence of printing texts and characters even in the absence of areas of intersection. The possibilities of forensic biological research using modern advances in mathematical modeling have been greatly expanded.

A forensic environmental assessment is also in the process of being formed today. Variants of classification of research objects depending on the place of the disaster (land, water, air), or on the type of catastrophes themselves (explosion, flood) are proposed. Recently, forensic environmental assessments are being carried out more and more often. They relate mainly to events such as the release of harmful substances into the environment and pollution of rivers and water bodies. More and more attention is being paid to the robots used in forensic activities. We offer our own version of the classification of robots by their role in the fight against crime: a) robots and robotic systems, functionally designed for the prevention, suppression, prevention of criminal attacks and administrative offenses; b) robots and robotic systems, functionally designed to study the situation of crimes committed and crime scenes.

III. CONCLUSION

We believe that "forensic robotics" is a branch of forensic technology that studies the practice of using special robotics in the process of suppressing, preventing, disclosing, investigating, preventing crimes and administrative offenses in order to develop recommendations on the design and modernization of robotic tools, as well as improving techniques, methods and methods of using these tools in order to optimize the establishment of objective truth in the case.

REFERENCES

[1] Hollegie, J.H.J. Basic Knowledge, document recognition, 2009, 232 p.

[2] Kelly, J.S., Lindblom, BS. Scientifi c Examination of Questioned Documents, Second Edition, CRC Press, 2006, 464 p.

[3] E. N. Bystryakov, I. V. Usanov Forensic robotics as a new branch of forensic technology.Research Journal №1(7) 2016 Criminal procedure, Criminalistics and Judicial examination Problems, c.17-22

DOI: https://doi.org/10.30837/IVcsitic2020201376

Information technology for the implementation of case-law management of end-to-end business processes

Serhii Chalyi[1]
[1]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, serhii.chalyi@nure.ua

Levykin Ihor[2]
[2]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, ihor.levykin@nure.ua

Abstract. *The problem of managing many end-to-end business processes is related to the distribution of common enterprise resources between them. This leads to delays in their implementation due to insufficient resources. The result of such delays can be a failure to complete the processes as a whole, which can lead to significant material financial losses. The management process consists in pausing or starting the execution of new processes based on formalized experience presented in the form of precedents. The main problem of the operational management of such processes is the timeliness of the development of their mathematical models. It is proposed to use models of analogue precedents with their subsequent adjustment to the parameters of the models of controlled end-to-end business processes. This process is implemented using Process Mining technology. To complete the stages of Process Mining, a generalized information technology has been developed for the case-based management of end-to-end business processes. Its implementation is connected with the simplification of case models of end-to-end business processes, the assessment of the lead-time of an end-to-end business process according to its current state, the adaptation of models of a set of ongoing processes, the integration of end-to-end business process models for a new order, and the management of ongoing and incoming new orders. This ensures their fulfillment within the deadlines established by the contracts.*

Keywords: *end-to-end business process, resources, precedents, operational management, information technology.*

I. Introduction and Problem statement

A lot of end-to-end business processes at the same time, they use the resources of the enterprise without the traditional restrictions imposed by its organizational structure. This leads to delays in their execution due to insufficient resources and to additional waiting for resources due to competition for them between processes. The result of such delays may be failure to comply with the restrictions on the execution time of the processes as a whole, which may lead to a decrease in the competitiveness of the enterprise and significant material losses.

As a result of this, the management of many end-to-end business processes is primarily associated with the distribution of the common resources of the enterprise between them. Obviously, processes use resources only during their execution. The management process consists in pausing or starting the execution of business processes in such a way as to efficiently distribute resources between them based on formalized experience, presented in the form of precedents.

The main problem of the operational management of end-to-end business processes competing for common resources is the timely development of their mathematical models.

II. Problem solution and Results

The solution to this problem is primarily associated with the presence of input and output data of the process, taking into account the influence of disturbances and the choice of control actions to achieve the desired result [1.2]. Therefore, it is proposed to use precedent models of analogues of such processes with their subsequent adjustment to the parameters of the models of controlled end-to-end business processes. This process is implemented using Process Mining technology [3].

To complete the stages of this technology, a generalized information technology of case-based management of end-to-end business processes is proposed, presented in the form of the following sequence of actions:

- Simplification of case models of end-to-end business processes, taking into account their current state;
- Estimation of the lead time of the end-to-end business process according to its current state;
- Adaptation of models of the set of processes performed;
- Integration of end-to-end business process models for a new order;
- Management of ongoing and incoming new orders.

Implementation of the action <Simplification of case models of end-to-end business processes taking into account their current state> is carried out taking into account one of its three states regarding the delay in their execution. The first condition of the PSU is characterized by the impossibility of its use in subsequent execution; the second state ensures the achievement of the target state with delays in the execution of the business process and the third state ensures the achievement of the target state without delay intervals. The simplification of the case model is supported by the appropriate method, which allows removing from the model those traces of the solution of the problem that do not further include the processing of objects by the name and values of their properties [4]. Метод включает в себя следующие этапы. 1. Формирование ограничений на новый бизнес-процесс. 2. Корректировка лога текущего бизнес-процесса. 3. Корректировка модели бизнес-процесса методами Process Mining. 4. Удаление интервалов выполнения действий и ожидания, не соответствующие полученной на этапе 3 модели.

The input for this action is: an event log that records all the actions in the corresponding database formed by the information system. Such databases contain information about

the precedent model of analogues and properties of objects (products, services). The procedure for obtaining the model of the current precedent, the formation, selection and adjustment of the analogue precedent model, carried out using the methods of the Process Mining technology [5].

After the step of obtaining a simplified precedent model of the analogue, carried out at the first stage of this technology, the process proceeds to the action <Estimation of the time to complete a business process by its current state>. The input of this action is a simplified precedent model of a business process and data on the duration of the intervals of waiting for its access to shared resources and runtime.

The execution of the <Estimation of the business process execution time by its current state> is carried out taking into account temporal restrictions imposed on the process. In this case, a subset of the possible trajectories of achieving the final state of the process of solving the problem of analyzing the data of both the event log and the model at the current time is determined. The duration of the execution is determined by the sum of the waiting interval and the execution time of the action for each trajectory of the process.

The implementation of this action is supported by the method of checking the implementation of temporal constraints, which includes the following steps. 1. The definition of a subset of the possible paths to achieve the final state of the business process. 2. Determining the time to reach the final state of the process relative to its current state for each trajectory of its execution. 3. The selection of a subset of options for solving problems for which the completion time of the business process does not exceed a predetermined threshold level. 4. Determination of the total duration of waiting intervals for each of the possible trajectories of the business process.

After receiving such an assessment, the transition to the action <Adaptation of models across the entire set of processes> is carried out. When this action is performed, by analogy with the first action, the current interval model of the set of processes is simplified (adapted) [6]. Those traces that will no longer be executed based on the previously selected trajectory determined during the execution of a particular process, taking into account the existing minimum and maximum intervals of the process, are deleted. The input of this action is the estimation of the process execution time by the current state and a database containing information on time intervals for all business processes that are performed. The result of this action is an adaptive interval model of a set of business processes.

Upon completion of the adaptation of models, the transition to the action <Integration of business process models for a new order> is performed.

The input for this action is: databases of orders, intervals of waiting for resources (equipment, technologies, personnel, materials, intervals of waiting for resources) and adaptive models of the set of processes being performed. The action is performed taking into account temporal constraints and the integration of models of a set of processes.

The result of this action is the refinement of the execution time of the new process by the waiting time of released resources with the calculation of the necessary time for its implementation and verification of the temporal restrictions imposed on it. The duration of the waiting interval is determined by the difference between the moment of generating a request for a resource for a new process and the moment they are released by executed processes. 5 After completing the previous action, the transition to the action <Management of executed and incoming orders> is performed.

The implementation of this action is carried out taking into account the assessment of the feasibility of the process and the imposed temporal restrictions. The way out are actions to manage ongoing and new orders.

This information technology supports the process of finding the necessary solution in the form of a sequence of priorities for the access of end-to-end business processes / orders to shared resources at all competitive points. The advantage of the technology is such an implementation of the process of finding the optimal sequences using the criteria of the remaining time and delay time for each business process, which ensures their implementation in a timely manner.

Its practical implementation is shown by the example of management of ongoing and incoming new orders. The process of finding the required solution consists in determining the optimal access orders to the common resources of 3 orders (Z) at 7 competitive points (CT), which is shown in Fig. 1.

This example shows all the possible and optimal sequences of the passage of orders at all competitive points.

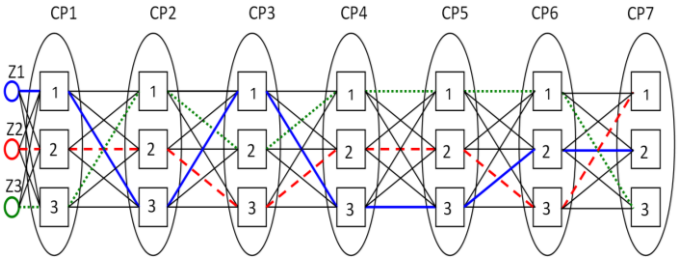


Figure 1. Sequences of orders of passage of orders of 7 competitive points

III. Conclusions

The proposed information technology for the process management of end-to-end business processes allows for the operational management of such processes based on the use of formalized analogue models. Their application ensures the implementation of many processes in accordance with the temporal restrictions imposed on them.

References

[1] Vom Brocke, J. (2015). Handbook on Business Process Management 1. Introduction, Methods, and Information Systems. Springer-Verlag Berlin Heidelberg, P. 709.

[2] W.M.P. van der Aalst. (2013). Business Process Management: A Comprehensive Survey. ISRN Software Engineering, 1-37..

[3] [3] Chalyi S.F. Razrabotka obobshchennoi protsessnoi modeli pretsedenta, metoda ego formirovaniya i ispol'zovaniya./ S.F. Chalyi, I. V. Levykin // zhurnal «Upravlyayushchie sistemy i mashinY». – USIM, 2016. № 3. Mezhdunarodnyi nauchno-uchebnyi tsentr informatsionnykh tekhnologii i sistem NAN i MON Ukrainy m. Kiev – pp. 23-28,

[4] [4] Chalii, S.F. Metod adaptivnogo protsesnogo upravlinnya na osnovi pretsedentnogo pidkhodu / S.F. Chalii, I.V. Levikin // Naukoємni tekhnologiї. – 2016. – № 4. – pp. 410-414.

[5] [5] Levykin, I.V. Metod sinteza tekhnologii process mining i sredstv imitatsionnogo modelirovaniya / I.V. Levykin // Tekhnologiya i tekhnika drukarstva KPI. – Kiev, 2016. – № 2 (52). – pp. 73-80.

[6] Chalyi S.F. Identification of the standby intervals in the business processes based on analysis of the sequence of events / S.F. Chalii, I.V. Levikin // Technology audit and production reserves. – 2016. – Vol. 5, N 2(31). - pp. 71-76.

DESIGN, IMPLEMENTATION AND OPERATION OF INFORMATION SYSTEMS AND TECHNOLOGIES

DOI: https://doi.org/10.30837/IVcsitic2020201438

Concept of Artifact-Event Description of Information System

Levykin Viktor[1]
Yevlanov Maksym[2]
Neumyvakina Olga[3]
Petrichenko Oleksandr[4]

[1] *Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, viktor.levykin@nure.ua*
[2] *Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, maksym.ievlanov@nure.ua*
[3] *Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, olga.neumyvakina@nure.ua*
[4] *Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, oleksandr.petrichenko@nure.ua*

Abstract. *The idea of artifact-event description of a web-based IS during its operation is formulated. Definitions of the concepts of "artifact" and "event" are proposed. Based on these definitions, the concept of an artifact-event description of IS during its operation was developed as a set of basic provisions on the basis of which models of web-based IS will be developed. The developed concept was the basis for a formalized description of web-based IS models set. The main dimensions, on the basis of which the formalization of the descriptions of the web-based IS and its elements, are allocated. A formalized description of the web-based IS models set and its elements is proposed, the main subsets of models forming this set are considered.*

Keywords: *information system, IT-service, artifact, event, model, commutative diagram.*

I. Introduction and Problem statement

Modern ideas about the life cycle of information system (IS) allow us to present the totality of the work of any particular IT company in the creation, implementation, maintenance and development of IS as a set of special cases of individual standard processes that are performed sequentially or parallel to each other. The connection between such processes is carried out through many artifacts, which are the results (outputs) of one process and at the same time the necessary information to start another process (inputs). However, it remains unclear today: is it possible to unify the presentation of such artifacts for IS for various purposes. Positive solution to this issue will significantly improve the efficiency and quality of management of IS life cycle processes by reasonably transferring the most successful management models, methods and practices identified on the basis of experience. Therefore, studies on the development of unified formal descriptions of IS and their elements are relevant not only from a theoretical, but also from a practical point of view.

Currently, two main ways of describing IS are used - architectural frameworks and visual modeling languages. However, both methods involve the conversion of one IS description into another based on a set of general or particular knowledge and rules. Analysis of modern systems description languages (for example, SysML [1]) and architectural frameworks (for example, TOGAF [2] or RM-ODP [3]) suggests that these rules can be implemented as follows:

- Particular rules for transforming one set of elements of visual models into another;
- Set of general rules establishing the architectural semantics of different languages;
- Set of general models and rules embodied in the form of a base or storage of IS artifacts.

Therefore, it is necessary to solve the problem of developing the concept of a formal description of IS and its elements, on the basis of which it will be possible to form similar sets of particular and general rules.

II. Problem solution and Results

Term "IS artifact" we will characterize that determinations:

- Description of a separate element of IS at different stages of its life cycle;
- Description of IS as a whole as an element of a larger system.

An event that occurs during the operation of an IS or its element we will be characterize as separate action from the set of permissible actions performed on one, several, or all artifacts of the IS and elements of this artifacts and leading to a change in the state of these artifacts.

Use of events to describe the behavior of IS allows us to formulate the concept of an artifact-event description of IS during its operation as a set of the following provisions:

- Any IS can be represented as a set of separate artifacts that establish the set of acceptable states of the IS and its elements, and the set of events that transfer these artifacts from one state to another;
- Any description of any IS artifact and event is an element of the universum, which includes both known and unknown to the Supplier, Consumer, or both of them IP artifacts and events, as well as methods for generating these artifacts and events;
- Any description of any IS artifact and event is considered as the initial variety of representations of the IS element at different stages of its life cycle at the level of data, information and knowledge;
- Any description of any IS artifact or event should be based on a process approach that defines the minimum process attribute model of IS element at different stages of its life cycle;
- Management of any IS artifact or event should be based on an approach based on the principle of gradually converting the set of initial attribute values describing this artifact or this event into the set of desired values of the same attributes.

In accordance with the service approach to the description of IS described in [4], it is proposed to use the following presentation levels of the operating IS:

- Level of managed objects and / or processes;
- System-wide level;
- IT accommodation (function) level;
- IT service level.

The concept of an artifact-event description of IS and its elements allows to distinguish the following levels of a formal description of an exploited IS:

- IS meta-metamodels level (a subset of artifact and event models);
- Level of IS metamodels (a subset of models of individual elements of IS and IS as a whole, based on an artifact-event description of IS);
- Level of IS models (a subset of the models of a particular operating IS and its individual elements formed on the basis of IS metamodels).

The need for a formal description at the same time according to the two dimensions highlighted above leads to a conceptual description of models set of operated web-based IS in the form of a two-dimensional matrix

$$M_{wIS} = \begin{bmatrix} M_{wIS}^{31} & M_{wIS}^{32} & M_{wIS}^{33} & M_{wIS}^{34} \\ M_{wIS}^{21} & M_{wIS}^{22} & M_{wIS}^{23} & M_{wIS}^{24} \\ M_{wIS}^{11} & M_{wIS}^{12} & M_{wIS}^{13} & M_{wIS}^{14} \end{bmatrix}, \quad (1)$$

where M_{wIS} – is many models of exploited web-based IS; M_{wIS}^{31} – is subset of artifact models that describe an abstract web-based IS as a single integrated IT product, and events that occur with these artifacts; M_{wIS}^{32} – is subset of artifact models describing an abstract web-based IS as a system consisting of personnel and complex automation, and events occurring with these artifacts; M_{wIS}^{33} – is subset of artifact models that describe an abstract web-based IS as a system of separate IT accommodation (function), and events that occur with these artifacts; M_{wIS}^{34} – is subset of artifact models that describe an abstract web-based IS as a system of separate IT services, and events that occur with these artifacts; M_{wIS}^{21} – is subset of models describing an abstract web-based IS as a single integrated IT product in terms of an artifact-event description; M_{wIS}^{22} – is subset of models describing an abstract web-based IS as a system consisting of personnel and complex automation in terms of an artifact-event description; M_{wIS}^{23} – is subset of models that describe an abstract web-based IS as a system of separate IT accommodation (function) in terms of an artifact-event description; M_{wIS}^{24} – is subset of models that describe an abstract web-based IS as a system of separate IT services in terms of an artifact-event description; M_{wIS}^{11} – is subset of models describing a particular exploited web-based IS as a single integrated IT product in accordance with metamodels M_{wIS}^{21}; M_{wIS}^{12} – is subset of models describing an abstract web-based IS as a system consisting of personnel and complex automation in accordance with metamodels M_{wIS}^{22}; M_{wIS}^{13} – is subset of models that describe an abstract web-based IS as a system of separate IT accommodation (function) in accordance with metamodels M_{wIS}^{23}; M_{wIS}^{14} – is subset of models that describe an abstract web-based IS as a system of separate IT services in accordance with metamodels M_{wIS}^{24}.

For matrix (1), the following condition is mandatory

$$\forall i = 1...4,\ j = 1...3, a = 1...4, b = 1...3, b \neq j$$
$$\exists M_{wIS}^{ij} \bigcap M_{wIS}^{ab} = \varnothing. \quad (2)$$

Depending on the approach to describing a web-based IS adopted at the stages of its creation and implementation, mappings forming commutative diagrams, can be defined on set (1). Example of this diagram is given below:

$$\begin{array}{ccccccc} M_{wIS}^{31} & \rightarrow & M_{wIS}^{32} & \rightarrow & M_{wIS}^{33} & \rightarrow & M_{wIS}^{34} \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ M_{wIS}^{21} & \rightarrow & M_{wIS}^{22} & \rightarrow & M_{wIS}^{23} & \rightarrow & M_{wIS}^{24} \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ M_{wIS}^{11} & \rightarrow & M_{wIS}^{12} & \rightarrow & M_{wIS}^{13} & \rightarrow & M_{wIS}^{14} \end{array}. \quad (3)$$

III. CONCLUSIONS

The proposed models set allows you to formally describe all the possible tasks that arise during the operation management of a web-based IS.

Given the developed formalized description of models set (1), it becomes possible to develop a model of an artifact, an elementary-single and scenario-single event. It is these models that are proposed to be considered as the main elements of a subset of artifact models that describe an abstract web-based IS as a system of separate IT services and events that occur with these artifacts. Further, it is planned to develop the transformation of these models into a subset of models that describe an abstract web-based IS as a system of separate IT services in terms of an artifact-event description, using the model IT-service model built using the Model-Control-View framework as an example.

REFERENCES

[1] F. Oquendo, J.C. Leite and T. Batista. Doftware Architecture in Action – Designing and Executing Architectural Models with SysADL grounded on the OMG SysML Standard. Undergraduate Topics in Computer Science. Springer. 2016. DOI: https//doi.org/10.1007/978-3-319-44339-3.

[2] "The Open Group Architecture Framework (TOGAF) – Core Concepts". Available at: http://www.togaf.org/togaf9/chap02.html#tag_03_01.

[3] ISO/IEC 10746-2-1996. Information Technology – Open Distributed Processing – Reference Model: Foundation. ISO/IEC Copyright Office, 1996.

[4] V.M. Levykin, M.V. Yevlanov, and M.A Kernosov. Pattern planning of requirements to the informative systems: design and application. Kharkov, Ukraine: Kompaniya «Smit LTD», 2014 (In Russian).

DOI: https://doi.org/10.30837/IVcsitic2020201439

Formation of Function Use Cases Based on Its Mathematical Model

Vasyltsova Nataliia[1]
[1]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, nataliia.vasyltsova@nure.ua

Panforova Iryna[2]
[2]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, iryna.panforova@nure.ua

Kuzma Yelyzaveta[3]
[3]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, yelyzaveta.kuzma@nure.ua

Abstract. *The analysis of modern research on the problem of formal description of scenarios for the fulfillment of functional requirements is carried out. The research problem is formulated as improving the accuracy of identifying precedents in descriptions of functional requirements. A technique to refine the description of a functional requirement has been developed. The proposed methodology was tested on the example of the function "Formation and maintenance of the individual plan of the department teacher". As a result of testing, the precedents of the function were clarified.*

Keywords: *Use Case diagram, functional requirement, case, mathematical model, individual plan.*

I. Introduction and Problem statement of the formation of function use cases based on mathematical model this function

Modern paradigm for describing system requirements is based on the publication of the requirements in the form of scripts. An example of the implementation of a given paradigm using visual models of the Unified Modeling Language (UML) is a model of the requirement provided by Microsoft Corporation [1]. Interest growth in research into the aspects of application of models for requirements engineering shows in [2]. One of area of this researches implies the development and improvement of models and methods of requirements engineering based on the identification and the formal description of knowledge from unstructured and weakly-structured texts. Thus, paper [3] discusses the issues on comparing and merging the elements of a system whose description are published in the form of Use Case diagrams, Activity diagrams, and data flow diagrams. Article [4] addresses the issue of converting the publications on requirements by rightsholders in an executable system model using behavior models by applying the Activity and State diagrams of UML. Solving the tasks on analyzing the requirements to IS, the description of which employed the UML class diagrams, was considered in [5]. Formal description of Use Case Diagram is given in [6].

However, the question remains open of how to highlight individual cases in the description of scenarios for fulfilling functional requirements. Existing recommendations do not allow us to formulate a general rule for the formation of precedents in the analysis of weakly-structured texts. Therefore, it should be recognized necessary to conduct a special study to find ways to identify cases in the description of the functional requirement scenario.

II. Problem solution and Results

The main problem of modeling precedents based on a textual representation of a subject area is the problem of blurred perception of individual fragments of this representation. Such a blur occurs due to the presentation of individual fragments of the text as separate precedents. This representation cannot be clarified until an analysis of the actions sequence of the investigated scenario is carried out.

To clarify textual representations in the process of collecting requirements, it is proposed to conduct a study of the structure of mathematical models describing the subject area. In the course of this study, it is proposed to describe each term or factor of the mathematical model, which has independent significance, with separate precedents on the Use Case diagram.

Most often, mathematical models of the subject area are presented in the form of equations or inequalities. Therefore, a study was conducted on the highlighting of precedents of the functions of the organization's management system based on text descriptions and mathematical models of these functions. As a result of the research, a technique for clarifying the description of a functional requirement is proposed. A generalized algorithm for performing this technique consists of the following steps.

Step 1. Separation of the document under study into its component parts.

Step 2. Designation of each part of the document as a separate element of the mathematical model and determination of the type of this model (additive or multiplicative).

Step 3. Analysis of the possibility of detailing the presentation of each element of the model as separate equation or inequality. If this is not possible, go to Step 5.

Step 4. Record detailed representations of the elements of the mathematical model and return to Step 3.

Step 5. Record the final presentation of the mathematical model of the document and highlight cases based on it. Clarify the previously highlighted list of cases. Completion of the algorithm.

Consider the application of this technique in the development of the functional task "Formation and maintenance of the individual plan of the department teacher". As a result of Step 1, it was found that subject area of this task can be represented by the "Individual Plan" document, which consists of six separate parts:

- position and stake;
- education work;
- educate-methodical work;
- scientific work;
- organizational and educational work;

– final distribution of time by type of work for the academic year.

During the implementation of Step 2, it was found that the last part of the Individual Plan document is an additive equation, which is a mathematical model of the remaining parts of this document. Therefore, the result of Step 2 is represented by the following equation:

$$\alpha_e C_e = T_1 + T_2 + T_3 + T_4, \quad (1)$$

where α_e – is part of teacher's rate; C_e – is quantity of hours allocated for one teacher's rate for the planned academic year; T_1 – is quantity of hours of education work planned for the academic year; T_2 – is quantity of hours of educate-methodical work planned for the academic year; T_3 – is quantity of hours of scientific work planned for the academic year; T_4 – is quantity of hours of organizational and educational work planned for the academic year.

During the implementation of Step 3 and Step 4 it was established:

- when planning education work, you should consider:
  - types of academic disciplines;
  - types of flows in which groups of students are combined;
  - types of academic work (lectures, practical exercises, laboratory work, etc.);
- when planning educate-methodical work, you should consider:
  - types of methodological work that must be performed for successful completion of the academic work;
  - types of methodological work that needs to be done to improve quality of academic work.

Therefore, (1) as a result of Step 3 and Step 4 was converted to the following equation:

$$\alpha_e C_e = \sum_{a=1}^{k}\sum_{b=1}^{l}\sum_{c=1}^{m} t_{abc} + \sum_{d=1}^{p_1} t_d + \sum_{f=1}^{p_2} t_f + \sum_{g=1}^{r} \frac{\alpha_g t_g}{q_g} + \sum_{i=1}^{s} t_i, \quad (2)$$

where t_{abc} – is quantity of hours of academic work that is planned to groups of students and to academic discipline; t_d – is quantity of hours of methodological work that is planned to successful completion of the academic work; t_f – is quantity of hours of methodological work that is planned to improve quality of academic work; t_g – is quantity of hours of types scientific work that is planned for the academic year; α_g – is planned number of results of the type of scientific work; q_g – is planned number of co-authors for the result of the type of scientific work; t_i – is quantity of hours of organizational and educational work that is planned for the academic year.

Equation (2) must be met subject to the conditions:

$$\begin{cases} 0 < \alpha_e \le 1; \\ t_{abc}, t_d, t_f, t_g, t_i, \alpha_g > 0; \\ q_g \ge 1; \\ t_{abc}, t_d, t_f, t_g, t_i, \alpha_g, q_g \in Z. \end{cases}, \quad (3)$$

As a result of Step 5, a list of the following precedents of the function under study was obtained:

- forming document section "position and stake";
- quantification of hours of education work planned for the academic year;
- forming document section "education work";
- quantification of hours of methodological work that is planned to successful completion of the academic work;
- quantification of hours of methodological work that is planned to improve quality of academic work;
- forming document section "educate-methodical work";
- quantification of hours of scientific work planned for the academic year;
- forming document section "scientific work";
- quantification of hours of organizational and educational work planned for the academic year;
- forming document section "organizational and educational work";
- forming document section "final distribution of time by type of work for the academic year".

III. CONCLUSIONS

The proposed technique allows to increase the accuracy of determining individual cases for describing scenarios for the implementation of functional requirements for IS. The consequence of applying this methodology in the process of collecting requirements from stakeholders will be a reduction in the number of errors in the identification of duplicate scenarios.

REFERENCES

[1] Modeling user requirements. Available at: https://docs.microsoft.com/ru-ru/visualstudio/modeling/model-user-requirements?view=vs-2015

[2] T. Ambreen, N. Ikram, M. Usman, M. Niazi. "Empirical research in requirements engineering: trends and opportunities," Requirements Engineering, vol. 23 (1), pp. 63–95, 2018. doi: https://doi.org/10.1007/s00766-016-0258-2

[3] H. Kaiya, K. Adachi, Y. Chubachi. 'Requirements Exploration by Comparing and Combining Models of Different Information Systems,' Knowledge-Based Software Engineering: 2108, pp. 64–74, 2019. doi: https://doi.org/10.1007/978-3-319-97679-2_7

[4] S.-K. Kim, T. Myers, M.-F. Wendland, P.A. Lindsay. 'Execution of natural language requirements using State Machines synthesised from Behavior Trees,' Journal of Systems and Software, vol. 85 (11), pp. 2652–2664, 2012. doi: https://doi.org/10.1016/j.jss.2012.06.013

[5] M. Ievlanov, N. Vasiltcova, I. Panforova. "Development of methods for the analysis of functional requirements to an information system for consistency and illogicality," Eastern-European Journal of Enterprise Technologies, vol. 1, no. 2 (91)), pp. 4–11, 2018. doi: https://doi.org/10.15587/1729-4061.2018.121849

[6] M.Q. Mohammed, S.Q. Muhamed, M. Ievlanov, Z. Gazetdinova. "Improvement of the method of scenario analysis of functional requirements to an information systems," Eastern-European Journal of Enterprise Technologies.vol. 3, no. 2 (99), pp. 25-35, 2019. doi: https://doi.org/10.15587/1729-4061.2019.170351

DOI: https://doi.org/10.30837/IVcsitic2020201440

The task of information system services integration

Yevlanov Maksym[1]

Sevostianova Kateryna[2]

[1]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, maksym.ievlanov@nure.ua*

[2]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, kateryna.sevostianova@nure.ua*

Abstract. *The urgency of solving the task of information system services integration is grounded. Rapid development of the market entails the need for each enterprise to be able to adapt the information system to changes in business processes. For successful integration of information system services on the level of business processes it is necessary to perform integration on the data level. The use of data integration systems is relevant to the integration of databases. The advantage of integration of information system at the data level is the low cost of integration.*

Keywords: *database, integration, information system, reengineering, service, functionality*

I. Introduction and Problem statement

At present, enterprises face the problem of integrating information system services, which are in different sources. The rapid development of the market entails the merger and consolidation of enterprises, which subsequently leads to the fact that the information system existing in the enterprise needs to be adjusted and adjusted to these changes. There is a need to quickly get access to integrated services of all organizations that are part of the enterprise. Thus, the approach to services unification by means of information system's data integration systems application is relevant [1]. There are a number of problems [2], which the developer of integration solutions faces, which can lead to information loss or significant losses, due to re-engineering of processes in the integration of key business processes of the company.

The issues of incompatibility of solutions of information system services integration tasks from different manufacturers were considered in [3]. The authors noted that process management solutions from one vendor do not interact with solutions from another, incompatibility of the presentation and format used by the vendors can hinder the interaction. They also noted that ISO 15746 standard can facilitate the task of integrating information system services. Based on the standard, they modeled the main components of the system using tools from different manufacturers, implemented information models and integrated the key functions of the system.

II. Problem solution and Results

There is a task "Formation and maintenance of an individual plan of a teacher". To solve this problem, a single database was created, which includes information about all types of teacher's work (academic work, scientific work, methodical work, organizational and educational work, as well as a list of positions and long-term assignments) and the load of the teacher.

There is a conceptual idea to create for each type of teacher's work, which is described in the individual plan of the teacher, a separate service - a micro-database, which will cover the functionality of this work. Thus, each section of the individual plan will represent a separate service of the information system. The resulting micro-databases should be integrated into a single database of the information system. At this level of integration, applications are configured to work with a single database. When using a single database for the information system services integration tasks, problems of data duplication or complexity of their extraction from hierarchical structures arise [4].

The obtained solution of an information system services integration task is to be compared in terms of adequacy with a database, which was obtained when solving the task "Formation and maintenance of an individual plan of a teacher".

III. Conclusions

The task of information system services integration at the moment is urgent, because the rapid market development leads to changes in information systems at enterprises. Development and maintenance of a fully integrated system is very expensive. The main problem of such systems is that when changing business processes at the enterprise it will be necessary to completely rebuild the system to meet the necessary requirements. The advantages of integration at the data level are low integration costs [5].

References

[1] Bukatov A.A., Pykhalov A.V. "Methods and means of integration of independent databases in distributed telecommunication networks", monograph, Southern Federal University, Rostov-on-Don, 2013, P. 160.

[2] Morozova O.A. "Integration of Corporate Information Systems", Moscow, 2014, P.140.

[3] Guodong Shao, Hasan Latif, Carla Martin-Villalba, Peter Denno. “Standards-based integration of advanced process control and optimization”. Journal of Industrial Information Integration, 2019, Vol.13, P. 1-12. doi:10.1016/2018.10.001.

[4] Dumchenkov I.A. "Review of methods of integration of information systems, their advantages and disadvantages", Young Scientist, 2018, Vol.23(209), P.176-177.

[5] Shchekochikhin O.V., Shvedenko P.V. "Analysis of Integration Levels of Heterogeneous Information Systems Components", Software Products and Systems, 2016, Vol .4 (116).

DOI: https://doi.org/10.30837/IVcsitic2020201441

Modern approaches of design software applications based on microservise architecture

Borysenko Viktor[1]

Borysenko Tatjana[2]

[1]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, viktor.borysenko@nure.ua*

[2]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, tetiana.borysenko@nure.ua*

Abstract. *The report covers modern approaches to improving the processes of creating Enterprise applications for complex business logic based on microservice architecture using a domain methodology.*

Keywords *design, software, Enterprise applications, Domain Driven Design, microservise architecture.*

I. INTRODUCTION AND PROBLEM STATEMENT

Microservices architecture has a positive impact on enterprise applications. Let's review general goals and principles for a microservice architecture (MSA). Here are the four goals to consider in Microservice Architecture approach [1-2]. Reduce Cost: MSA will reduce the overall cost of designing, implementing, and maintaining IT services.

Increase Release Speed: MSA will increase the speed from idea to deployment of services.

Improve Resilience: MSA will improve the resilience of our service network.

Enable Visibility: MSA support for better visibility on your service and network.

At the same time microservice architecture follow basic principles:

- Scalability;
- Availability;
- Resiliency;
- Flexibility;
- Independent, autonomous;
- Decentralized governance
- -Failure isolation;
- -Auto-Provisioning;
- -Continuous delivery through DevOps/

Business logic implements business rules is the base part of the enterprise applications. The development of an application with complex business logic is a complicated and time-consuming process.

At the same time, designing and implementation of complex business logic for applications are based on microservice architecture is harder than for monolithic applications. The main reason is the requirement to split the whole logic effectively between different microservices.

The typical domain model looks like a spiderweb of interrelated classes. To build complex software applications based on the microservice architecture it is required to solve two essential problems.

The first problem is that hierarchy of classes in microservice architecture should be split by services, unlike monolithic architecture. Therefore, first of all, it is necessary to get rid of the objects' references that cross boundaries of services.

The second problem lies in the design of the business logic that is restricted by the usage of transactions in a microservice architecture.

II. PROBLEM SOLUTION AND RESULTS

The current work uses the modern methodology of domain-driven design (DDD) as a fundamental approach for developing enterprise applications [3]. This approach includes firstly usage of strategic and secondarily tactic design patterns.

Basic concepts of domain-driven design using strategic templates [4]:

- Single language;
- Limited context;
- Subject domain,
- Subject subdomain;
- Semantic core;
- Context map.

Strategic design patterns are used in different modern enterprise applications as building blocks. Some of them are supported by such frameworks as JPA and Spring. To achieve strategic development is enough to use such tools.

It is proposed to use the base pattern "Aggregate" in this work that is one of tactical design patterns used in DDD methodology. It structures the business logic as a set of aggregates. These building blocks are very useful during development of microservices.

The domain model describes a set of classes and the relationship between them in traditional object-oriented design. Classes are usually grouped into packages. The boundaries between different business objects are not clear in the traditional domain model. Such ambiguous vague separation may cause problems, especially in microservice architecture.

The lack of clear boundaries also causes problems when updating a business object in addition to conceptual uncertainty. A typical business object has invariants, i.e. special business rules that must always be followed. But for observance of invariants it is necessary to carefully design business logic.

Changing or updating parts of a business object directly may result in violation of business rules. "Aggregate" as tactical pattern of DDD methodology helps to solve this problem effectively.

In this case, the aggregate is the cluster of domain objects that can be used as unified whole. It consists of a root entity, as well as one or more entities and objects. Many business objects are designed as aggregates. For example, "Gas transportation" subject domain contains some nouns like "Gas pipeline section", "Compressor yard ", "Compressor station" are aggregates.

The “Aggregate” pattern creates a business model in the form of a set of aggregates, i.e. graphs of objects that can be used as a unified whole. Structuring the domain model as a set of aggregates defines clear boundaries.

Aggregates break down the domain model into blocks and it’s easier to design them individually. They also determine the scope of operations, such as updating, fetching, and deleting.

The aggregate is often loaded from the entire database, it allows to avoids any problems with lazy loading.

When an aggregate is deleted from the database all its objects are deleted too.

Updating the whole aggregate, and not its individual parts, solves problems with consistency as described in the previous example. Update operations are called for the root of the aggregate, which ensures the observance of invariants.

In addition, in order to maintain competitiveness, the aggregate root is blocked by version number or database isolation level. However, it should be mentioned that this approach does not require updating the entire aggregate in the database.

Another rule that aggregates must obey is that a transaction can only create or update one aggregate. This limitation is ideal for microservice architecture. It ensures that the transaction does not overstep the limits of the service. It also agrees well with the limited transnational model of most NoSQL databases.

It is important to decide how big it is necessary to make this or that aggregate during developing a domain model. On the one hand, ideally, aggregates should be small.

This will increase the number of simultaneous requests that your application is able ot handle and improve scalability as each aggregate's updates are serialized.

This will also have a positive effect on the experience of interaction, as it reduces the probability that two users will try to make conflicting changes to the same aggregate.

But on the other hand, an aggregate is the scope of a transaction, therefore, in order to ensure the atomicity of a certain update, on the contrary it is worth making it larger.

The negative aspect of large aggregates in the context of microservice architecture is that they prevent decomposition. For example, the business logic for orders and customers should be in the same service, which makes this service more volumetric. Considering these problems it is better to make aggregates as small as possible.

The main part of the business logic consists of aggregates in a standard microservice. The rest of the code belongs to domain services and narratives.

Narratives orchestrate local transaction chains to ensure data consistency.

Services serve as entry points of business logic and are called by inbound adapters.

The service uses the repository to retrieve aggregates or save them to the database.

Each repository is implemented by an outgoing adapter that accesses the database.

In the context of DDD, a domain event is something that happened with an aggregate.

In a domain model it is a class. An event usually represents a state change. In this work, it is recommended to use the “Domain Event” template - the aggregate publishes a domain event at the time of its creation or during some other significant change.

The usefulness of domain events relates to the fact that other parts of the interaction (users, external applications, or other components within the same application) are often interested in information about changes in the state of the aggregate.

A domain event is a class with a name based on the passive participle of the past tense. It contains properties that expressively describe this event. Each property is either a simple value or an object.

A domain event usually has metadata, such as its identifier and timestamp. It may carry the identifier of the user who made the change, as far as it is useful for audit. Metadata can be part of an event object - possibly defined in the parent class. Or they can be inside the wrapper around the event object. The identifier of the aggregate that generates the event may also not be its direct property, but it can be part of the wrapper.

But the disadvantage of requesting an aggregate from a service is the additional costs of fulfilling this request. Alternatively, you can use event enrichment.

It means that events contain the information that a consumer needs. As a result, event consumers become simpler because they no longer need to request data from the service that posted the event. Event enrichment simplifies consumers, but the drawback of such approach is the risk of violation of open/closed SOLID principle for event classes.

These classes can potentially be changed each time when clients’ requirements are changed. This can adversely affect support of event as such kind of changes can affect several parts of the application.

Earlier, the main reasons why aggregates are suitable for developing business logic in a microservice architecture were presented.

When an aggregate is created or updated it must publish domain events. These events have many implementation areas. Subscribers of domain events notify users and other applications, as well as publish messages in a client browser via WebSocket.

III. CONCLUSIONS

A good way to organize the business logic of a microservice is to split it into aggregates according to the DDD principle. Aggregates make the domain model more modular, exclude the possibility of using object references between services and ensure that each ACID transaction is performed within the same service.

REFERENCES

[1] Irakli Nadareishvili, Matt McLarty, Michael Amundsen/ Microservice Architecture: Aligning Principles, Practices, and Culture/- O'Reilly, 2016.-144

[2] Kasun Indrasiri, Prabath Siriwardena. Microservices for the Enterprise.- Apress, 2018.- 434 p.

[3] Vijay Nair. Practical Domain-Driven Design in Enterprise Java - Using Jakarta EE, Eclipse MicroProfile, Spring Boot, and the Axon Framework.-Apress, 2019.- 388

[4] Chris Richardson. Microservices Patterns: With examples in Java. Manning Publications: 2018.- 522Felipe Gutierrez. Introducing Spring Framework.-Apress:2014.-352

DOI: https://doi.org/10.30837/IVcsitic2020201443

Reengineering technology of specialized information systems

Chyrkova Kateryna

Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, kateryna.chyrkova@nure.ua

Abstract. *The subject of research is the process of reengineering the automated working places of specialized information systems of an organization. The technology of reengineering of specialized information systems is offered, which consists in the choice of organizational and technical structure of working places of staff taking into account the influence of the degree of automation of project decisions on the performance indicators of the organization. The use of the developed technology makes it possible to make rational choice of design solutions to increase the degree of automation of working places, which ensures improvement of the performance indicators by maximizing the completeness and reliability of data entry in the conditions of uncertain reengineering costs.*

Keywords: *specialized information system; automated working place; degree of automation; reliability of data; completeness of data; reengineering of information system.*

I. Introduction and Problem statement

One of the mechanisms for improving the performance of the organization, and thus maintaining competitiveness is the development of an information system that provides information support for the business processes of the organization. Information systems provide data collection and data processing during the execution of business processes with varying degrees of automation, which affects the completeness and reliability of information of business processes information support. The completeness and reliability of data collection and processing is particularly critical for specialized information systems in which information support affects the quality of the end result, for example, related to human biological and infectious safety.

Accordingly, such specialized information systems need to be upgraded or reengineered in order to improve the indicators that evaluate the performance result of the organization. The need for reengineering or upgrading of specialized information of the system can be caused by the emergence of new vectors of development of the organization, the emergence of new regulatory requirements for business processes and new information technologies, the presence of initial errors in the design of specialized information system.

II. Problem solution and Results

At present, there are several concepts: reengineering, modernization, migration, evolution, restructuring of the information system, which in one way or another determine the improvement of the current information system [1].

Much attention is paying to the study of methods, models and technologies of reengineering or upgrading information systems that include the relevant phases or steps [2]. At the same time, there are no generally accepted methods, models and technologies of reengineering of specialized information system, which would provide determination of rational variant of organizational and technical structure of working places taking into account influence of degree of automation of workplaces on indicators of activity of organization and uncertainty of spending resources on reengineering.

The following technology is proposing for reengineering of specialized information system:

– decomposition of business processes of the subject area;

– decomposition of specialized information system into automated working places [3];

– determining the degree of automation of each working place [4];

– formation of datasets of information support of business processes with appropriate degrees of automation [5];

– identifying performance indicators that are affected by the completeness and reliability of the data collection;

– expert evaluation of the importance of datasets;

– determining the importance of each working place;

– formation of a table of impact of datasets on certain performance indicators of the organization;

– analysis of the functional structure of the specialized information system for compliance with the established requirements and standards;

– formation of many alternative variants of design decisions for working places;

– determination of partial performance indicators of each working place under the respective variant of the design decision and costs for modernization;

– selection of rational organizational and technical structure of the each working place according to the criterion [6].

III. Conclusions

It is advisable to use the proposed technology of reengineering of the specialized information system to increase the performance of the organization by modernizing the organizational and technical structure of the automated workplaces in the conditions of unspecified reengineering costs.

References

[1] Yu. V. Doronina, V. O. Ryabovaya, “Metod modernizatsii informatsionnyih sistem ekologicheskogo monitoringa na osnove analiza ih funktsionalnoy nagruzki,” Tr. SPIIRAN, vol 44, 2016, pp.133–152.

[2] М. С Сафонов, “Метод реінжинірингу інформаційної системи з використанням об’єктів управління,” Електротехнічні та комп’ютерні системи, vol 13, 2014, pp. 105-113.

[3] А. В. Міхнова, Д.К. Міхнов, К.С. Чиркова, “Метод формування організаційно-технічних структур сегментів ІС служби крові,” зб. наук. пр. Системи обробки інформації. – 2015. – № 12 (137). – С. 156–160.

[4] A. Mikhnova, D. Mikhnov, K. Chyrkova, “Information support model of production transfusion processes,” Eastern-European Journal of Enterprise Technologies, vol. 3/3 (81), 2016, pp. 36–43. DOI: 10.15587/1729-4061.2016.7167.

[5] А. В. Міхнова, Д.К. Міхнов, К.С. Чиркова, “Модель спеціалізованої медичної інформаційної системи,” *Вісник Кременчуцького національного університету імені Михайла Остроградського. Кременчук:* КрНУ, vol 5(118), 2019, pp. 75–82. DOI: https://doi.org/10.30929/1995-0519.2019.5.75-82.

[6] A. Mikhnova, D. Mikhnov, K. Chyrkova, “Method for evaluating the efficiency of upgrading specialized information systems,” Innovative technologies and scientific solutions for industries, vol. 4 (10), 2019, pp. 69-76. DOI: https://doi.org/10.30837/2522-9818.2019.10.069.

DOI: https://doi.org/10.30837/IVcsitic2020201444

Implementation of a monitoring system in an automated fare collection system

Budko Anna[1]
[1]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, anna.budko@nure.ua

Shapa Lyudmila[2]
[2]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, liudmyla.shapa@nure.ua

Partyka Stanislav[3]
[3]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, stanislav.partyka@nure.ua

Abstract. *This article describes the benefits of implementation of a monitoring system in an automated fare collection system and suggests some methods for its implementation.*

Keywords: *automated fare collection system, monitoring system, TMS, GSM.*

I. Introduction and Problem statement

Nowadays, monitoring information systems are often used to obtain not only statistical information, but also for subsequent processing of this information. In particular, such systems are being actively implemented in public transport, because public transport monitoring can reduce costs of using public transport and if it is necessary reorganize public transport movement to improve service quality and road safety [2-4].

II. Problem solution and Results

The implementation of a monitoring system in an automated fare collection system of public transport will allow:

1. Generate a history of movement for each vehicle and save this data to the archive.
2. To collect statistics on mileage, speed and perform the calculation of the average fuel consumption.
3. Organize control of which users and organizations can view information of monitoring system and carry out transactions.
4. Carry out messaging with drivers, control the situation on the road and predict delays.
5. Prohibit the misuse of public transport.
6. Inform about various target events.
7. Collect statistics on movements with subsequent transfer to the accounting system and analysis.
8. Control of working hours, including continuous driving of one driver.
9. Speed monitoring.

Also, additional functions will become possible due to sharing TMS modules with the monitoring system. For example, it will be possible to compare the actual movement of the public transport with the planned route or to inform about events such as deviation from the route, fuel drain, engine shutdown, etc.

To relieve the operator from the need to constantly monitor the status of transport in the online mode, in the TMS monitoring module can be implemented the ability to generate messages to the operator about different events on the road. But this requires the installation of additional sensors, on the basis of which information will be generated, such as accurate fuel gauges, opening or closing doors, temperature control etc.

Control over the actions of drivers will lead to a reduction in GSM costs by 10-15%, which will cover the cost of GPS monitoring services.

The monitoring system can be implemented using a GPS module integrated in an automated fare collection system. This will expand the capabilities of AFC system, which in turn has everything necessary to receive, store and process the necessary information about the transaction. Then it can transfer all the necessary information to the processing center, where real-time information processing will be recorded.

According to the research work [1] bandwidth consumption with the available public transport mode for a month is not more than 50 megabytes, which is 9% of the total traffic for the transmitting GPS coordinates.

The obtained data can either be accumulated in a GPS tracker or in on-board computer and then transferred to a central base, or transmitted to a central server in real time mode to a processing center.

Nevertheless, it is necessary to comprehensively study the effectiveness of implementing public transport monitoring. It is also necessary to provide competently administrative management of the monitoring system and ensure the security of information in the monitoring system, because intruders can use it for their own purposes.

III. Conclusions

Thus, the implementation of a monitoring system in an automated fare collection system will provide many advantages that can improve public transport system to a new level of service.

Using monitoring systems allows to collect data from devices with one or more communication servers, Then it redirects databases to the main server and distribute them between connected intermediate servers that will provide user interaction or performing background tasks. Such a construction of the monitoring system will allow users from different regions to work with the closest regional web server with a minimum delay to it.

References

[1] Yeromina N. S., Shapa L. S., Budko A. O. “Using of global positioning system navigation services in automated fare collection systems”, CSITIC, pp. 51–52, April 2018.

[2] Guilin L. D., Zhang J. Z. Shaohua C. Vehicle Monitor System for Public Transport Management Based on Embedded Technology, Physics Procedia, vol. 24, pp. 953-960, March 2012.

[3] Martovitskii, V. A., Ruban, I. V. Model' mul'tiagentnoi sistemy sbora i khraneniya informatsii. Sistemi upravlinnya, navigatsiї ta zv'yazku, (6), 150-153.

[4] Martovytskyi V. O. Arkhitektura multyahentnoi systemy monitorynhu rozpodilenykh informatsiinykh system / V.O. Martovytskyi, K. R. Lokotetska // tezy dopovidei KhXVII mizhnarodnoi naukovo-praktychnoi konferentsii MicroCAD-2019, 15-17 travnia 2019 r.: u 4 ch. Ch. IV «Informatsiini tekhnolohii: nauka, tekhnika, tekhnolohiia, osvita, zdorovia». – Kh. : NTU «KhPI», 2019. – S. 164.

DOI: https://doi.org/10.30837/IVcsitic2020201445

Analysis of Accelerated Problem Solutions of Word Search in Texts

Zaiceva Sofia[1]

Barkovska Olesia[2]

[1,2]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, olesia.barkovska@nure.ua

Abstract. *The work is devoted to the topical problem of word search in texts, the implementation of which is essential in such tasks as electronic dictionaries formation, digital libraries creation, data compression, forecasting algorithms etc. The main problem faced by the majority of scientists who work on this issue is the speed of the existing algorithms implementation. In the work, the existing algorithms speed analysis was conducted and realization by means of a hybrid computer system was proposed.*

Keywords: *word pattern, parallelizing, high-performance computing system, Boyer-Moore algorithm.*

I. Introduction and Problem statement

Continual accumulation of information results in an increase of the information volume in electronic information resources (IR) warehouses. This does not complicate information processes connected with data mining, exchange, accumulation, storage, retrieval and transfer, however, this inhibits accomplishment and implementation time increment of such information processing operations as the given information search [2] and processing due to the growth of the number of computing operations necessary for the solution of the problem of information search in IR storages. Numerical, textual, graphical, audio and video data are distinguished according to the way of information representation. We will focus on the study of textual information being the kind of information represented in the form of written text, i.e. in the form of a predetermined sequence of symbols, because any kind of text analysis [1] (morphological, syntactical and semantic) is applied in a wide variety of applied fields such as marketing and market research, mass media and social networks monitoring, tonality analysis as well as opinion, feedback and complaints rating, for the search of answers to questions received by call-centers, for possible events forecast, in security systems, enabling to lock transfer of unwanted or sensitive information through the Internet etc.

All the above-mentioned types of text analytics and its areas of application explain the relevancy of developing methods of accelerated text search in large input text data arrays by means of the review and adaptation of the existing traditional methods of data mining for shared memory parallel computing systems and massively parallel systems.

II. Problem solution and Results

Among the existing algorithms of word pattern search in texts, the following algorithms are extensively used and have the given performance: linear search ($O((t-l)\times l)$), Aho-Corasick, Boyer Moore ($O(t/l)$), Knuth-Morris-Pratt ($O(t+l)$) and Rabin-Karp ($O((t-l)\times l)$) algorithms, in which t is the source text length, l is the search word length.

With regard to the given performance, Boyer Moore and Knuth-Morris-Pratt algorithms were adapted in the work for massively parallel systems.

Distribution of source text among shared memory computers and application of the fork-join program model supported by Boyer Moore algorithm provide for the rapid (where t=18589 and l=9, the search time for search word is 3,56ms) and almost error-free (0,018%) word pattern search in the text.

A large amount of computers available in massively parallel systems and GPGPU concept utilization with the application of Knuth-Morris-Pratt algorithm enable rapid (where t=18589 and l=9, the search time for search word is 1,85ms) almost error-free (0,084%) word pattern search in the text.

III. Conclusions

Analysis of the obtained results showed that an increase in the number of search words is followed by an increase in the search time as well as an increase in search time is caused by an increase in the source text size.

Application of shared memory multiprocessors enables to acceleration of up to 90 times while massively parallel systems provide for the acceleration of up to 135 times.

References

[1] Data Science & Big Data Analytics: Discovering, Analyzing, Visualizing and Presenting Data/ EMC Education Services. David Dietrich, Barry Heller, Beibei Yang. Published by John Wiley & Sons. Inc. USA, 2015. 435 p.

[2] 1. Barkovska O.Ju., Pyvovarova D.I., Serdechnyj V.S., Ljashova A.O. Pryskorenyj alghorytm poshuku sliv-obraziv u teksti z adaptyvnoju dekompozycijeju vykhidnykh danykh (Advanced Algorithm of Word Patterns Search in Texts with Adaptive Output Decomposition). // Systemy upravlinnja, navighaciji ta zv'jazku. – Poltava: PNTU, 2019. – Issue №. 4(56). – pp.28-34

[3] Najma Sultana, Sourabh Chandra, Smita Paira, Sk Safikul Alam. A Brief Study and Analysis of Different Searching Algorithms // 2017 SECOND IEEE INTERNATIONAL CONFERENCE ON ELECTRICAL, COMPUTER AND COMMUNICATION TECHNOLOGIES – 2017. – P. 944-948.

DOI: https://doi.org/10.30837/IVcsitic2020201446

Hybrid language processing approach

Havrashenko Anton[1]
[1]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, anton.havrashenko@nure.ua

Barkovska Olesia[2]
[2]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, olesia.barkovska@nure.ua

Abstract. *Creating a computer system for translating text from hybrid languages into any arbitrary language is a challenge not only for our country. The global trend of borrowing words from other languages is spreading rapidly and leading to the emergence of new so-called "mixed" languages. We propose an algorithm for constructing a dictionary and presents translation results that show up to 65% translation accuracy.*

Keywords: *translator, programming language, internet, dictionary, text processing.*

I. Introduction and Problem statement

In the modern world, there are a large number of different languages that can be mixed, to borrow foreign words, leading to the emergence of so-called hybrid languages and slang. Slang - very informal language that is usually spoken rather than written, used especially by particular groups of people[1]. Online translators like Google, Yandex can translate only around 100 literary languages. In addition, adding new words for translation is usually impossible, which is not enough in the modern world.

Today, there are no specialized translators available for translating slang or hybrid languages, but their number is constantly increasing. Previously, new slangs were born during the influence of neighboring countries upon them and depended on a particular territory or among people of a particular profession. But they were quite similar to the original, with the addition or change of not usually a large number of words. Nowadays, slang is formed under the influence of a certain book, movie, game and may not be understood by a stranger.

This causes the relevance of the algorithm for constructing the dictionary to translate text from hybrid languages and slang into existing languages of the world, and also developing a “mixed language translator” application based on the proposed algorithm.

II. Aims and tasls of the work

The main purpose of the project is to implement processing of the input text, turning it into a dictionary and the opportunity to use this dictionary to translate.

To achieve this goal, the following tasks must be solved:

- create an algorithm for constructing dictionary to translate text from hybrid languages and slang existing world languages;
- developing a “mixed language translator” application based on the proposed algorithm.

III. Problem solution and Results

To accomplish these tasks, a software package of 10 programs was developed:

№1 - Initial Text Processing; №2 - bilateral improve processing dictionary; №3 - improving translation of similar languages by the n-gram algorithm;[2] №4 - improving translation of similar languages by Knut-Morris-Pratt algorithm;[3][4] №5 - search phrases, phraseology and translation for them; №6 - a combination of 2 words in one language[5] №7 - build vocabularies in other languages and improve vocabularies using already built ones; №8 - supplementing the finished dictionary with other texts; №9 - splitting the dictionary into dictionaries with a small percentage of text intersection; №10 - translator.

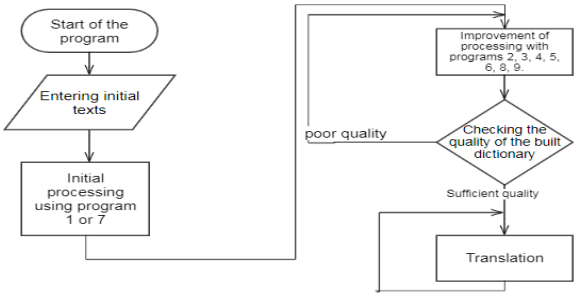


Figure 1. Flowchart of the algorithm

The algorithm have the following structure. Programs 1 and 7 are input and are only used for initial word processing. All programs except 1, 7, and 10 improve the dictionary until the required quality of the dictionary is reached. After achieving the required quality, the dictionary is transmitted to the translator program, which interacts with the user translating the input data.

IV. Conclusions

There is potential for further work on the system. During the testing, no critical errors were detected at any of the stages of operation.

For further development, it is suggested to consider the problem of changing the translation by re-entering the same data and entering incorrect data. Also possible to develop the idea of common vocabulary that is stored on a server and the translation via the Internet.

References

[1] Cambridge Dictionary [Electronic resource] URL: https://dictionary.cambridge.org/dictionary/english/slang

[2] N-gram [Electronic resource] URL: https://uk.wikipedia.org/wiki/N-грам

[3] Prefix function. Knut-Morris-Pratt algorithm [Electronic resource] URL:https://e-maxx.ru/algo/prefix_function

[4] S. Aygün, E. O. Güneş and L. Kouhalvandi, "Python based parallel application of Knuth-Morris-Pratt algorithm," 2016 IEEE 4th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE), Vilnius, 2016, pp. 1-5.

[5] Kevin McTait, Arturo Trujillo. A Language-Neutral Sparse-Data Algorithm for Extracting Translation Patterns. Proceedings of 8th International Conference on Theoretical and Methodological Issues in Machine Translation, August 1999, Chester, UK

DOI: https://doi.org/10.30837/IVcsitic2020201447

Software-hardware Complex of Access Control and Management

Lytvynenko Vladyslav[1]
Ivashchenko Heorhii[2]

[1]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, vladyslav.lytvynenko@nure.ua
[2]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, heorhii.ivashchenko@nure.ua

Abstract: *The presented work is dedicated to the issues of development software-hardware complex of access control and management based on Arduino platform. The hardware part of the complex works together with the web-application, created using React, Redux, Node.js and MongoDB technologies. This provides extensive functionality of the application.*

Keywords: *access control, RFID, Node MCU, React, Node.js, MongoDB.*

I. INTRODUCTION AND PROBLEM STATEMENT

In commercial and industrial settings, the issue of access control of identified individuals to various buildings and premises is one of a high-priority. The possibility of control comprises the prevention of access by the mechanism responsible for the functions of locking and unlocking.

Management of access control system allows to change the privileges of selected individuals and record all attempts of entrance. The use of RFID tags, which may be implemented in different formats, became a common method of user identification.

Comparison of existing systems of access control and management (SACM) revealed a range of their drawbacks: high cost, limited functionality, inability to save data on the personal server, limited ability to activate/deactivate access keys without rewriting software, complicated management of users' RFID tags status.

II. PROPOSED SOLUTION

The solution of the issue of access control and management is development of competitive software-hardware complex, which provides versatility, as well as the ability to broaden functionality.

Proposed solution is based on the use of hardware platform Arduino. Module RC522 is used to read data from an RFID tag. NodeMCU platform is used to process and send RFID tag data to the server. This platform is also a controlling mechanism (with the use of switching relay and solenoid) for granting access. This platform represents a board for development based on ESP8266 (version ESP12E) and includes UART-Wi-Fi module with low energy consumption [1].

Performance of switching relay and solenoid depends on power availability, in the case of absence of which, the complex is not able to function properly and remains in a closed state. This allows to prevent trespassing onto a premises by shutting down the power grid.

Web-application is used for managing the hardware part of the complex, server side of which is responsible for the business logic of SACM solution, and is implemented on a programming platform Node.js using Express framework [2]. Interaction with the hardware part takes place with the help of HTTP request that is sent from Node MCU platform to the server, which processes received data and sends back a response. The use of Node.js platform together with Socket.io library provides convenient application of WebSocket communications protocol, which allows transferring data from the server without waiting for a request from the client side.

Data is saved by means of non-relational database management system MongoDB, to work with which ODM (Object Data Modelling) library Mongoose is used. This ensures safety, simple integration and high productivity of data manipulation [3].

Client side is implemented in the form of an SPA-application, by means of which administrator can control access and view logs by graphic interface [3]. Administrator can add new users to the system and change status of existing RFID tags, which have been used at least once for an attempt of entrance. The developed solution allows to collect data about all entrance attempts regardless of their result or whether the users are in the database and export of data in CSV format for further processing.

Client side was created with the React library, used for making user interfaces and intended to solve issues of partial renewal of web-page content [4]. For controlling the state of the developed SPA-application, React is used in combination with Redux library. Redux enables saving the state of the whole application in the tree of objects in a single storage.

III. CONCLUSIONS

The developed solution for access control and management encompasses software part and hardware part. Software part is in the form of a web-application which combines simple graphic user interface, support of necessary functionality and the possibility of its expansion. Hardware part is implemented on NodeMCU platform containing a microcontroller, Wi-Fi module, which is well suited for creating Internet of Things.

Using the suggested complex will provide the flexibility of setting access modes, logging and controlling working hours, higher level of safety and a possibility to receive information regarding whether employees adhere to the work schedule or not.

REFERENCES

[1] M. Jayakumar, “The internet of things with esp8266 Hands on approach: Get started with Arduino IDE and ESP8266,” CreateSpace Independent Publishing Platform, 2017, 270 p.

[2] G. Lim, “Beginning Node.js, Express & MongoDB Development,” Independently published, 2019, 151 p.

[3] H. San, “MongoDB Best Practices: Build Fault Tolerant Applications,” Kindle Edition, 2014, 131 p.

[4] A. Banks, E. Porcello, “Learning React: Functional Web Development with React and Redux,” Apress, 2017, 350 p.

DOI: https://doi.org/10.30837/IVcsitic2020201448

Methodology Approach to Choosing a Cloud Platform

Sayenko Vladimir[1]

Pavlenko Marko[2]

[1]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, vladimir.sayenko@nure.ua, l*

[2]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, marko.pavlenko @nure.ua*

Abstract. *Modern information systems today necessarily use cloud resources. But there is still the problem of choosing the best platform for remote access to computing resources. The following is a methodology approach to choosing a Cloud platform and provides recommendations for how to choose one of them. The methodology is based on the use of a specific system of criteria, the values of the estimates of these criteria and estimates of weighting factors of significance.*

Keywords**:** Cloud Platforms, computing resources, criteria, estimation, AWS, Google Cloud platform, Microsoft Azure.

I. Introduction and Problem statement

Nowadays, the modern information systems necessarily use the cloud resources.

This concept provides for remote processing and storage of data. It gives Internet users access to the server's computer resources and to the software services as an online service. That is, if you have an Internet connection to the Cloud, you can perform complex calculations, process data using the power of a remote server. And you don't have to buy the right hardware. It is sufficient only to get the Internet connection.

The demand for such resources is huge. More and more offers appear on the market. Choosing a particular cloud service provider is an urgent task. This task is especially important for new pilot projects and start-ups.

Nowadays, there are many available efficient services in the cloud services market. A big world leader companies and small firms use these services today. Cloud platforms are not the same and differ in conceptual approach, set of provided services, prices, etc.. But, owners of Cloud services perform roughly the same actions - providing these services for free or for a fee. These services cover access to powerful computing resources, software, related technical documentation, and recommendations how to use all of the services.

Thus, we can distinguish the problem of choosing the best cloud platform for our needs. The choice is complicated because there are a lot of Cloud services in today's IT market. They have different characteristics and prices of services. But they are open for investigation and discovering to get the best solution and to find the best choice of the usage [1].

II. Problem solution and Results

In order to choose the best cloud platform, all the financial, functional and technical requirements for the project should be defined and prioritize all needs.

The leaders of the modern European and American markets, which fully meet all the requirements of the basic criteria, can be called platforms from Amazon (AWS), Google Cloud and Microsoft Azure [2, 3, 4]. It should be noted that in the Asian market, the main leader is Alibaba Cloud (included in the holding of Alibaba Group).

It is proposed to perform the following three steps to choose a cloud platform: 1) Identify technologies; 2) Price and pricing model; 3) Evaluation of platforms by special criteria.

A. Description of the methodology.

The methodology involves a two-stage assessment. The first stage is a preliminary assessment. The second stage is a detailed assessment.

The first stage includes four steps: 1) Definition of technologies, 2) Cost models; 3) Compatibility with general requirements 4) Compatibility of the project with available specialists. At this stage we determine a quality estimation.

The second stage includes a detailed assessment of 6 criteria. At this stage we determine a quantity estimation. For each of criterion we use a significance coefficient and special expert evaluation.

B. Description of the first stage

1) ***Identify technologies***. We need to determine what technologies, protocols, programming languages are required to complete your project. Do not consider platforms that do not provide these capabilities. Although today almost all platforms support services for all software platforms. There are only some differences in stability and reliability.

2) ***Cost models.*** In most cases, customers choose the financial and resource model of payment - it reflects the financial impact of resources on the service, which is more in line with the economic nature of cloud services. It takes into account not only the maximum number of virtual resources of the cloud platform (systems, clusters), but also other expensive equipment, that requires to be.

In general, the pricing model is the exchange process where the client/end-user pays for the services offered by the cloud provider.

Table 1. Cost models

Provider	Cost model
AWS	Fee per hour / week for resource use. Fee for temporary / permanent data transfer, GB.
Google Cloud	Fee for basic kit by developer or professional (data transfer, resources, consultation of technicians, etc.)
Microsoft Azure	Fee per hour / week for computing capacity and for temporary / permanent storage of GB of data in storage

Cloud service providers have 2 main pricing models: static and dynamic. In the first case, the price remains unchanged after its determination, in the second case it changes

dynamically according to the availability of resources, demand and so on.

Among the main fixed or variable factors that affect pricing in cloud providers are the following:

- Quality and cost of service;
- Investment amount (provider costs for cloud services)
- Lease contract term;
- Reputation of cloud users and providers.

3) ***Compatibility with general requirements***. When developing systems, there are often requirements for compatibility of the developed system with existing ones and compatibility with customer requirements. A typical example - for many solutions, it may be the best option - choose AWS, but there is the same requirement to choose only MS Azure.

4) ***Compatibility of the project with available specialists.***

An important aspect when choosing a cloud platform is the availability of certified specialists for a particular platform. The more certificates and the higher the rank of certificates could help to choose the more compatibility cloud platform.

C. Description of the second phase

5) ***Evaluation of platforms by special criteria***

a) Physical protection. This requirement is mandatory for any cloud platform, as the threat of cyberattacks is constantly increasing. For the protection, new and updated security tools are being added: unique scanning anti-virus programs and password encryption mechanisms in the database, bit-based data encryption in both parties, activation of server and client authentication and more

b) Legal protection. It will also be necessary to ensure not only that there is sufficient information but also legal and legislative protection of their data by the chosen platform. To do this, you need to carefully study and analyze the information regarding the Territorial Data Centers (TDC) in your country and the cloud platform you have chosen. It is recommended that all actions are complied with the European Package of Standards for Personal Data Protection

c) No hidden costs. As of 2019, about 75% of large corporations, small and medium-sized businesses, are experiencing financial problems: the difficulty of backing up, leasing space for equipment, inefficient use of resources, unauthorized use by employees of cloud-based competitors. Because of this, the overhead of platform maintenance is rising and companies are having to implement various hidden taxes.

d) Backuping and recovering of information. You need to know how often data is backed up, or if there is any mechanism in place. Each platform provides its own information recovery solution. Although each of them has many small details and features, there are fundamentally two approaches. This is done through stand-alone (database servers) or cloud-based virtual repositories.

e) Supporting. If you are planning on long-term use, you must ensure that the platform provides high-quality advice from highly qualified specialists. That you can get such help on a wide variety of technical issues, schematics and models for any possible transfer of projects to other platforms. Also you get clearly described documentation for setting your software up for any operating system..

f) Possibility of integration. The best way to get started with cloud technology and optimize existing resources is to use a hybrid cloud environment. Hybrid integration solutions provide API support and enterprise connectivity, allowing applications, data and processes to be integrated quickly and easily. The best of hybridity is implemented in Microsoft Azure [6]

III. PROBLEM SOLUTION AND RESULTS

The following is a table of the cloud platform assessments of the offered criteria, and the coefficient of significance of each of the criteria in a specific example.

Table 2. Example

Factors	AWS	Google Cloud	Azure
No hidden costs Significance coefficient 0.8	7	8	8
Physical protection Significance coefficient 0.9	8	9	9
Legal protection Significance coefficient 0.8	9	9	9
Backuping and recovering of information Significance coefficient 0.7	7	9	8
Supporting Significance coefficient 0.6	8	8	6
Possibility of integration Significance coefficient 0.5	8	7	9

All estimates (weights) and significance factors are expert and for each individual case they will be individual. Table 2 shows an example of criteria evaluation and decision making. Let we have a result of expert evaluation for all 6 factors. For each factor, its own significance coefficient was chosen. For each cloud platform was determined the weight.

The sum of the values of the criterion scores, which are multiplied by the significance factor, we obtain the following average scores: AWS - 32.9 points, Google Cloud - 36.3 points, Azure - 35.4 points. Google Cloud Service Providers dominate the average Azure margin and AWS by a significant margin. However, if any of the evaluation criteria is not essential to a particular project, its coefficient may be reduced, the estimates re-listed and another platform selected.

IV. CONCLUSIONS

A methodology for evaluating the feasibility of using a cloud platform is proposed. It could be used in the implementation of a project for the development of information systems. The methodology is based on the use of a specific system of criteria, the values of the estimates of these criteria and estimates of weighting factors of significance. The proposed methodology does not provide accurate estimates and can serve as a starting point for the final decision on the choice of a cloud platform.

REFERENCES

[1] Bogdanov, A.V. The comparison of several cloud computing platforms /A.V. Bogdanov, E. Mint. Ning; UDK 519.687.7. – Rel.№2, ser. №10. – St. Petersburg: Herald SPbSU, 2013. — 9c.

[2] Amazon Web Services: AWS Documentation. URL: https://docs.aws.amazon.com/.

[3] Google Cloud Platform: GCP Documentation. URL https://cloud.google.com/docs/

[4] Microsoft Azure: Azure Documentation. URL: https://docs.microsoft.com/en-us/azure/.

[5] The cloud battle: Google vs. Microsoft vs. Amazon. URL: https://enonic.com/blog/cloud-battle-google-microsoft-amazon

DOI: https://doi.org/10.30837/IVcsitic2020201449

Investigation of maximum overheating device dependence on its size and installation density

Semenets Valerii[1]
[1]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, e-mail: valery.semenets@nure.ua

Sinotin Anatoly[2]
[2]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, e-mail: anatolii.sinotin@nure.ua

Sotnik Svetlana[3]
[3]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, e-mail: svetlana.sotnik@nure.ua

Abstract. *The theses show the results of influence studies of heated zone volume of an electronic device on its maximum overheating.*

Keywords: *heated, zone, anisotropy, thermal conductivity, conductive, heat sinks, coefficient, heat.*

I. Introduction and Problem statement

The design of modern devices, along with the development of electrical circuits, requires strict consideration of temperature regime of future design. This poses a challenge for designer to carry out thermophysical design at all stages of development of reliable, economical, small-sized radioelectronic equipment (REE). An attempt to empirically search for an acceptable variant of constructions becomes economically unjustified.

Incorrect placement of one element can be easily detected and eliminated in process of temperature testing (verification calculations) of finished design. The elimination of errors in general layout of elements requires additional overhead for processing the entire design of apparatus. This poses before designer the task of ensuring the normal thermal regime of elements at all stages of apparatus development.

Purpose of study is establishing the nature of apparatus size influence on temperature regime of created design.

Formulation of problem. Literary sources on thermophysical design of REE with a given thermal regime are represented mainly by journal articles. The main developments are aimed at selection and optimal use of air cooling systems. Monographs on general design of REE provide only verification calculations of temperature fields.

Thermophysical design is carried out on basis of multiple calculations for various parameter values, i.e. trial and error method is used. This work presents the results of study of heated zone shape influence on maximum overheating of apparatus.

II. Problem solution and Results

The effect of apparatus volume on maximum overheating of instrument can be expressed in terms of so-called initial parameter F_0

$$F_0 = \frac{P_0}{\vartheta_0} \cdot \frac{1}{4\lambda \cdot \sqrt[3]{V}} \cdot \frac{0{,}82A_0^3}{3\mu_0^2}; \quad (1)$$

$$Bi_0 = \frac{K_0}{\lambda_0} \cdot \frac{1}{2} \cdot \sqrt[3]{V}, \quad (2)$$

where P_o – total power of heat sources, W; ϑ_o – maximum permissible overheating of device, degrees; λ_o – effective heat conductivity in absence of heat sinks with gas filler, W/m · deg; V_0 – volume of heated zone, m^3; A_o, μ_o – amplitude and eigenvalues of characteristic equation for B_{I_o}; K_o – average surface heat transfer coefficient W / m^2 · deg.

The initial parameter F_o characterizes the thermal regime of following REE design:

– heated zone is in form of a cube $(\xi_{X_o} = \xi_{Y_o} = \xi_{Z_o} = 1)$, where

$$\xi_{I_o} = 2l_{mii} / 2l_i, i = X, Y, Z; \quad (3)$$

– there is no anisotropy in thermal conductivity in volume and heat transfer on surfaces $(\lambda_X = \lambda_Y = \lambda_z = \lambda_o; K_X = K_Y = K_Z = K_o)$;

– conductive heat sinks are absent $(\lambda_{max} = \lambda_o)$;

– power of heat sources is evenly distributed.

In Fig. 1 shows dependence of parameter

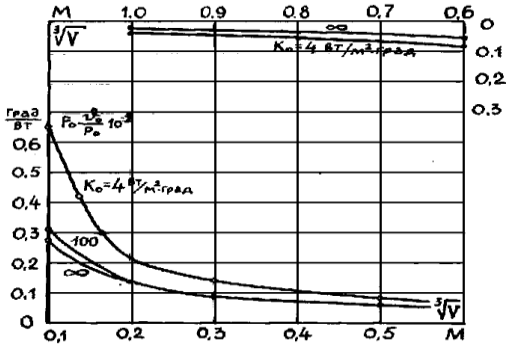


Figure 1. Dependence of initial parameter F_o on dimensions of heated zone and intensity of surface heat exchange K_o at $\lambda_o = 0{,}2\ W/m \cdot \text{deg}$.

$F_o \cdot \vartheta_o / P_o \cdot 10^2$ from volume of device heated zone and heat transfer coefficient K_o characterizing the surface cooling system for devices with effective thermal conductivity $\lambda_o = 0{,}2\,W/m \cdot deg$ [1]. From graphs it follows that initial parameter F_o allows minimizing by reducing the ratio P_0 / ϑ_0, increase in volume of heated zone V and the intensity of surface heat transfer K_o.

Consider each factor individually. The decrease in ratio P_0/ϑ_0 causes certain requirements for development of an electric circuit of apparatus.

For implementation of circuit solutions, it is advisable to choose an element base with lowest power consumption and materials with high temperature resistance. If it is necessary to use individual elements with a low permissible superheat temperature ϑ_o, it is advisable to separate these elements into an independent group so as not to complicate the provision of a given thermal regime of device design as a whole. This remark is very important to take into account when choosing the elemental base of electric circuit, since after setting the electric circuit designer, it is not possible to influence the dissipated power factor and temperature resistance of circuit elements.

An analysis of dependences (Fig. 1) shows that for single-block cubic structures of apparatus with a size of $\sqrt[3]{V} \geq 0{,}5$ m, minimizing the initial parameter Fo due to an increase in volume of heated zone (density of elements) and transition to a more intense surface cooling $K_0 = \infty$ system becomes almost impossible.

Conversely, for structures of size $\sqrt[3]{V} \leq 0{,}5$ m, an increase in volume and growth K_o leads to a three-fold decrease F_o at $\sqrt[3]{V} = 0{,}1$ m and by 50% at $\sqrt[3]{V} = 0{,}3$ m due to a change K_o from 4 W / m^2 · deg to ∞. Practically already at $K_o \geq 100$ W / m^2 · deg, limiting case occurs, that is, for devices with gas filling (with low effective thermal conductivity $\lambda_o = 0{,}2$ W / m · deg), it is inexpedient to use liquid and other more efficient surface cooling systems [2, 6].

Extreme minimization F_o can be achieved through use of forced convective air cooling (α =10–100 W / m · deg) [3, 4].

Heat transfer coefficient

$$K_o = \frac{K^1 S_k / S}{1 + K^1 S_k / \alpha S}, \qquad (4)$$

where K_o – heat transfer coefficient through gas gap from heated zone to casing, W / m^2 · deg;

α – heat transfer coefficient between surface of casing and environment, W / m^2 · deg;

s_K, s – surface area of casing and the heated zone, m^2.

An analysis of expression (4) and values of heat transfer coefficients for various types of cooling systems [3, 5] allows us to outline two ways of increasing K_o to minimize parameter F_o and synthesize structure with a given thermal regime for maximum overheating. The first way is purely constructive at low values K_o, i.e., for electronic devices designed to function in conditions of natural cooling by air

Calculations of a large number of instrument designs [2, 7] showed that there is equality of conductivities between heated zone and the casing, as well as with environment:

$$K^1 \cdot S \approx \alpha \cdot S_K \qquad (5)$$

After substituting (5) in (4) we obtain, $K_o = \alpha \cdot S_K$ i.e. use of a casing almost 2 times reduces the efficiency of surface cooling.

When combining casing of apparatus with heated zone, $(S_K = S)$, $K^1 \to \infty$ and $Ko = K$.

Thus, in a purely constructive way, combining instrument cover with heated zone, K_o it can be doubled (Fig. 2) In this case, it is necessary to ensure good thermal contact between heated zone and casing, for example, using high-conductive pastes in joints between boards (chassis), casing faces, etc. The considered method is most effective when it is necessary to maintain tightness (dustproof) equipment.

You can go in another constructive way: to reduce influence of casing on intensity of heat sinks due to violation of tightness and ensuring direct contact of heated zone with

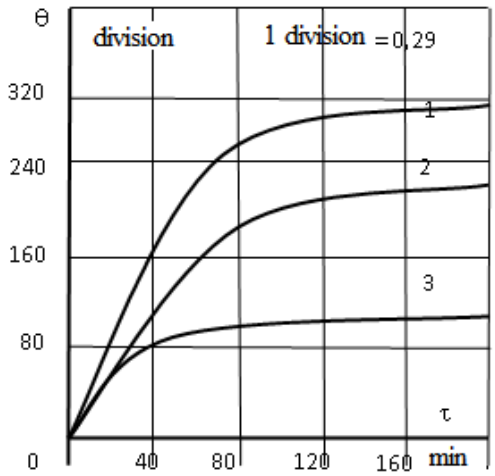


Figure 2. Temperature at the center point heated zone. 1 – in absence of heat sinks; 2 – in presence of heat sinks;3 – at conclusion of heat sinks to casing.

DOI: https://doi.org/10.30837/IVcsitic2020201455

cooling air through perforation (blinds) openings. Then expression for K_o in first approximation takes form

$$K_0 = K^{\bullet}{}_0(1 + S_{пер} / S_{k)}, \quad (6)$$

where $S_{пер.}$ – area of perforations, m^2; K_0 – is determined by expression (6) at $S_{пер.} = 0$. The ratio $S_{пер.} / S_K$ is called perforation coefficient. A more rigorous account of perforation is given in [3]. Almost already at $S_{пер.} / S_K$ = 0.5–0.6, value K_0 is close to K_o^* that is, limiting effect of minimization F_o is achieved.

The considered constructive methods do not allow significant changes in heat transfer coefficient. For a significant change in intensity of heat transfer on surface of heated zone, a transition from natural to forced surface cooling by blowing air is necessary, that is, additional changes in design of apparatus are required.

In this case, according to equality (2), it is necessary either to simultaneously increase the heat transfer intensity between heated zone and casing (K^1), casing and environment (α), or first to combine casing with heated zone $(K^1 \to \infty)$. Otherwise, the growth Ko will be insignificant, despite a significant increase α. Thus, in second way of minimizing due to increase K_o, transition to a new cooling system is foreseen with preliminary combining of casing with heated zone, especially in tight-fitting constructions.

An increase in volume of heated zone due to a decrease in density of elements is in conflict with requirement to minimize size of structure, therefore it can only be applied when there are no strict restrictions on size of structure in technical task.

In practice, a change in volume by a factor of 8 (in area $\sqrt[3]{V}$ <0.5 m) leads F_0 to a three-fold decrease at K_0 = 4 W / m· deg and a half-time decrease $K_0 = \infty$ (Fig. 2). Such a change in volume can be accomplished by switching from high density $(\eta_м \geq 1)$ mounting to low mounting $(\eta_м \approx 1)$.

III. Conclusions

1. It is established that transition to construction in form of a square "bar" provides most effective minimization of shape parameter. The degree of minimization increases with increasing efficiency of apparatus cooling system

2. Effective minimization of initial parameter can be carried out for apparatus designs with a linear size of less than 0.5 m, due to transition to a low density or to increase the efficiency of surface cooling system. For structures with a linear size of more than 0.5 m, minimizing initial parameter is almost impossible.

References

[1] Н. А. Ярышев, "Расчёт температуры однородного объекта при конвективном теплообмене", Изв. вузов. Приборостроение, 2000, Т.43, № 4, С. 61.

[2] В. И. Шелест, А. С. Кондрашов, "Концептуальный алгоритм теплофизического проектирования радиоэлектронных средств", Технология и конструирование в электронной аппаратуре, 2003, № 5, С. 26 – 27.

[3] И. С. Кондрашов, "Моделирование тепловых режимов активных компонентов электронных модулей", Технология и конструирование в электронной аппаратуре, 2006, № 2, С. 43 – 44.

[4] Т. А. Исмаилов, Ш. А. Юсуфов, "Температурное поле электронной платы внутри герметичного радиоэлектронного блока кассетной конструкции", Изв. Вузов. Приборостроение, 2004, Т. 47, № 7, С. 21 – 25.

[5] В. В. Семенец, А. М. Синотин, Т. А. Колесникова та ін. "Исследование зависимости максимального перегрева радиоэлектронного аппарата от его параметров", Системи обробки інформації, 2018, №4, С. 29–34.

[6] Т. А. Колесникова, В. В. Семенец, А. М. Синотин, "Исследование температурных полей РЭА методом регулярного теплового режима", II Міжн. нук.-техн. конф. «Виробництво & Мехатронні системи» (M&MS-2018), Харків, 2018, С. 63–65.

[7] В. В. Семенець, А. М. Сінотін, Т. А. Колесникова, "Проектування одноблокових радіоелектронних приладів із заданим тепловим режимом" : Монографія, Харків: ХНУРЕ, 2006, 172 с.

DOI: https://doi.org/10.30837/IVcsitic2020201450

Algebraic Approach to the Description of Temporal Knowledge in Decision Support Tasks

Levykin Viktor[1]

Chala Oksana[1]

[1]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, viktor.levykin@nure.ua*

Abstract. *The problem of automated construction of a temporal knowledge base for supporting decision-making in solving partially structured and unstructured organizational management problems is considered. The solution to this problem is associated with the formalization of temporal relations, reflecting the implemented sequence of control actions. The formal description should take into account not only the relationship in time between control actions, but also the static dependencies between the structural elements of the organizational management object, represented by the organizational structure of the object. An algebraic approach to the description of temporal knowledge is proposed. According to this approach, common temporal rule is defined. The rule determine the relationship in time between facts. Each logical fact is knowledge about the state of the control object at a certain point in time. The rule establishes temporal dependencies for time-consistent facts, as well as for facts, which are true at certain intervals. The proposed algebraic approach makes it possible to combine temporal relations that reflect the control process with dependencies, taking into account the structure of the control object.*

Keywords: *management decision, decision support, temporal relationship, state of the control object, algebraic approaches.*

I. Introduction and Problem statement

Decision support is used to solve partially structured and unstructured tasks at the tactical and strategic levels of organizational management. Such support is carried out in order to form a management decision for atypical states of the control object. The specified solution is implemented in conditions of incomplete information about the current state and includes a sequence of control actions that ensure the transition from the current to the target state of the control object.

The sequence of management decision involves solving the problems of finding the set of possible sequences of control actions, as well as implementing the selected decision. The first task involves the subtasks of detecting and analyzing the anomalous state of a management object, as well as generating many alternative options for executing a management decision. Solving the sub-problem of constructing multiple alternatives requires considerable resources. This determines the importance of using the decision support system in solving this problem. The second problem is solved directly by a decision-maker and combines the choice of one of the alternatives and the implementation of the selected decision.

The search for managerial decisions is usually implemented in decision support systems [1] using a knowledge base. Existing approaches to construction a knowledge base in such systems are based on the use of communicative methods for extracting knowledge. These methods provide for the formalization of the knowledge necessary to support decisions based on the results of a dialogue with experts in a selected subject area [2]. However, communicative methods are time-consuming. It does not allow timely to obtain an up-to-date knowledge base in the event of an evolutionary change in approaches, methodologies and technologies that are decisive in the activities of the enterprise. Such a development of technology is characteristic of modern innovative enterprises, for example, in the field of software development for information systems.

To overcome the key disadvantage of traditional approaches to construction a knowledge base, it is advisable to use temporal relations instead of causal ones [3]. The latter determine the temporal ordering of control actions. Therefore, they can be obtained on the basis of the analysis of the sequence of actions as part of the implemented management decisions. Such an opportunity creates the conditions for the automated construction of temporal knowledge bases in decision support systems [4, 5].

The relevance of the research topic is related to the fact that solving the problem of automated formation of a knowledge base based on the analysis of temporal ordering of known sequences of control actions requires the construction of a formal basis for describing temporal knowledge. The specified description should reflect both the temporal relationship between the control actions and the static dependencies represented by the organizational structure of the control object.

The purpose of the report is to construction a formal description of temporal knowledge in order to provide the possibility of the formation and verification of many alternative options for managerial decisions in the form of time-ordered sequences of control actions.

II. Introduction and Problem statement

Algebraic approaches to the description of algorithms and information technologies have found application in improving the structure of software systems in order to increase their speed, as well as identifying deadlock states.

An algebraic description of knowledge, including the rules of inference, makes it possible to formalize the processes of building and expanding the knowledge base in decision support tasks. Such a description contains algebraic structures represented by a set with relations defined on it. The first, a static relation, defines the basic, unchanging relationships between the elements of the set. The second relationship determines the dynamics of change in the implementation of organizational management.

The developed algebraic description of temporal knowledge reflects the many states of the control object, as well as the hierarchical and temporal relations between these states.

The state of a control object at each time is determined by a finite set of attributes A. The typed values of each element

DOI: https://doi.org/10.30837/IVcsitic2020201455

$a_k \in A$ are given by a finite set $V_k = \{v_{k,l}\}$. The acquisition of a variable a_k the value $v_{k,l}$ within the proposed description of temporal dependencies is displayed as an elementary fact $\varphi_{k,l}$.

Every fact Φ_j, that reflects the state s_j of a control object at a point in time τ_j, is given in the representation of temporal knowledge through conjunction of elementary facts $\varphi_{k,l}, k = \overline{1,K}$. If all the facts $\varphi_{k,l}$ are true at a point in time τ_j, then the fact Φ_j is also true:

$$\Phi_j = \begin{cases} true\ if\ \exists \tau_j : \forall k\ \varphi_{k,l} = true, \\ false\ otherwise. \end{cases} \quad (1)$$

The set $\Phi = \{\Phi_j\}$ is partially ordered by the moment τ_j of truth of these facts. Facts reflecting one alternative sequence of control actions Π_i are linearly ordered in time. Facts belonging to different sequences Π_i may not have temporal relationships.

Each pair of facts (Φ_j, Φ_m), pertaining to one alternative is always associated with a temporal relation. Such a pair of ordered facts in the knowledge base seems to be a temporal rule.

The first fact is the antecedent of the rule and determines the state of the control object, which is a condition for the implementation of the temporal rule. The second fact is a consequence of the rule. Consequence defines a control action and its results as a new state of the control object. The state s_m, is reflected by the fact Φ_m. Accordingly, the application of the temporal rule changes the set of facts that are true at the current time. The relationship between the facts is set by the temporal operator $o \in O$ and temporal quantifier.

Temporal operators O determine the set of possible temporal relationships between facts. For example, a fact Φ_m must definitely become true immediately after the fact has become true Φ_j. Or else the fact Φ_m will be true sometime in the future after the fact Φ_j.

The sequence of revealing the true facts, applying the temporal rules, as well as forming a new list of the true facts is the basis of a direct output on the temporal rules. The result is a sequence of states of a management object, or a sequence of control actions within a management decision.

Static structural dependencies between facts are determined by the set H of operators of union, intersection, and fact difference. For graphical representation of these operators are used traditional signs of combination, intersection of sets: $\{\cup, \cap, \setminus\}$.

The union of facts Φ_j, Φ_m is performed when they determine the status of the individual components of the control object. The condition of a control object as a whole is generally determined as a union of these facts:

$$\Phi_j^{(1)} \bigcup \Phi_j^{(2)} = \left(\bigwedge_{k: a_k \in A_1 \cup A_2} \varphi_{k,l} \right) \Big| \tau \geq \tau_j^{(1)}, \tau \geq \tau_j^{(2)}, \quad (2)$$

where τ – current time, A_1, A_2 – sets of attributes that determine the state of the control object represented by facts $\Phi_j^{(1)}$ and $\Phi_j^{(2)}$, respectively.

According to (2), the united fact will be true when the last of the facts $\Phi_j^{(1)}$, $\Phi_j^{(2)}$ is true.

The intersection and difference of facts is defined similarly.

In general, the union and intersection of logical facts makes it possible to use «bottom-up» and «top-down» approaches to construct a hierarchical representation of temporal knowledge.

Algebraic description $\mathcal{R}$ of temporal knowledge for decision support tasks consists of a basic set of facts, as well as relationships that determine the static and dynamic relation between these facts:

$$\mathcal{R} = \{\Phi, O, H : \forall (\Phi_j, \Phi_m) \in \Phi\ \exists (o \vee h)\}, \quad (3)$$

where Φ – set of facts Φ_j, that describe state of the control object; $o \in O$ – temporal operator that determines the type of temporal relationship between the facts; $h \in H$ – set of relationships that allow you to determine the hierarchy of these facts, including the organizational structure of the control object.

III. CONCLUSIONS

A generalized description of temporal knowledge is proposed. The description defines the time dependencies between the facts presented in the form of temporal rules. Each fact corresponds to the knowledge of the condition of the control object at a certain point in time. The state of a control object is defined by set of values of variables that describe that object. Each rule establishes temporal relations for a pair of facts. These facts can be true both consistently over time and at intervals.

In practical terms, the proposed algebraic approach makes it possible to take into account the following features of the use of knowledge to support decision-making: the application of personal knowledge of performers in addition to the formal knowledge describing the behavior of the control object; multi-level organization of knowledge, reflecting the organizational hierarchy of the control object; expansion knowledge as the management process is implemented.

REFERENCES

[1] C.K. Oduoza. “Decision support system based on effective knowledge management framework to process customer order enquiry”, in Chiang, S. Jao(Eds), Decision Support Systems, INTECH, Croatia, 2010, p. 406.

[2] K. Dalkir “Knowledge Management in Theory and Practice”, Burlington, Massachusetts: Elsevier Butterworth-Heinemann, 2005, 372 p.

[3] V. Levykin, O. Chala “Method of determining weights of temporal rules in markov logic network for building knowledge base in information control system”, EUREKA: Physics and Engineering, 2018, №.5, pp. 3-10. DOI: http://dx.doi.org/10.21303/2461-4262.2018.00713.

[4] V. Levykin, O. Chala (2018). Method of automated construction and expansion of the knowledge base of the business process management system. EUREKA: Physics and Engineering, 4, 29-35. doi: 10.21303/2461-4262.2018.00676.

[5] Levykin, V., Chala, O. (2018). Development of a method for the probabilistic inference of sequences of a business process activities to support the business process management. Eastern-European Journal of Enterprise Technologies, 5 (3 (95)), 16–24. doi: https://doi.org/10.15587/1729-4061.2018.142664

DOI: https://doi.org/10.30837/IVcsitic2020201452

Principles of explanation in e-commerce system based on sales dynamics

Leshchynskyi Volodymyr[1]
Leshchynska Irina[2]

[1]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, volodymyr.leshchynskyi@nure.ua
[2]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, iryna.leshchynska@nure.ua

Abstract. *The problem of forming explanations to the recommendations of items in the electronic commerce system is considered. The principles of constructing explanations that take into account changes in demand for goods and services are proposed. The first principle involves the use of a quantitative indicator as an explanation for a recommended subject. The second principle is associated with an iterative refinement of this quantitative indicator when recording new information about the choice of users in the database of the e-commerce system. The third principle postulates the use of implicit feedback from the user to construct explanations. As this feedback, information on sales of items is used, since this information is confirmed by the payment of users. The developed principles make it possible to formulate an online-explanation for the recommendations received, taking into account current data on sales of goods or services.*

Keywords: *recommendations, explanations, recommender subsystems, personalization of sales, e-commerce.*

I. Introduction and Problem statement

E-commerce systems have gained significant competitive advantage over traditional offline channels because they provide support for consumer choice through advisory subsystems [1]. Such support is realized by creating a personalized list of recommended objects, taking into account the interests of the particular consumer.

Recommendations use information about the selection of products and services by users with similar preferences. Similarity of preferences is established on the basis of comparison of the goods and services sold to these consumers. The use of recommendations greatly simplifies consumer choice, which has led to an increase in the popularity of e-commerce systems.

In order to increase user confidence in the proposed list of goods and services, the recommendation may be supplemented by an explanation [2]. Explanations allow the user to simplify their selection of products from the recommended list, reduce time spent buying goods and services, which in turn leads to increased sales in the e-commerce system.

Explanations increase customer loyalty in the case of inaccurate recommendations that do not fully meet consumer preferences. The reason for the inaccuracy of the recommendations is the irrelevance of the ranking of goods and services in the recommended list due to incomplete information about the interests of the consumer or about the characteristics of the goods.

The first case is characteristic of the cold start of the recommendation subsystem. The recommendation subsystem perceives the new user as "cold" because it has no information about the history of its choice and therefore cannot determine its preference for goods and services [3].

The second case usually occurs as a result of user shilling attacks. Such attacks are intended to increase sales of the target assets and reduce sales of competitors' products. To achieve this, information on product ratings is distorted through the use of fake user profiles [4]. Personalized recommendations after a shilling attack contain a list of objects that are fit for the purpose of the attack.

However, these recommendations do not take into account the interests of real buyers of goods and services. As a result, confidence in the e-commerce system is diminished, which may reduce demand for goods and services.

Existing approaches to explanatory formation are a further development of methods for explaining the results of logical inference in expert as well as precedent systems. These approaches are complemented by the criteria for evaluating explanations. Compliance with the above criteria makes it possible to increase sales of goods and services [5].

However, it should be noted that existing approaches to constructing explanations do not consider changes in consumer interests and characteristics of objects over time. A temporal model that integrates such changes integrally is proposed in [6], but the issues of using this model to form explanations need further consideration.

Thus, the problem of developing explanatory principles based on the dynamics of sales of goods and services needs further research.

II. Problem solution and Results

The suggested explanatory principles in the e-commerce advisory subsystem take into account changes in user demand over time. In particular, the increase in demand for a particular product can be an explanation for users regarding the popularity and high consumer characteristics of the product compared to competitors' products.

This approach should consider the criteria for evaluating changes in user choice, changes in sales resulting from the use of explanations [6].

The proposed principles of explanatory construction include:

- a quantitative assessment of the explanation for each recommended item;
- iterative clarification of explanations in order to take into account changes in consumer preferences over time;
- the use of implicit user feedback.

The first principle corresponds to a set of criteria for evaluating changes in user choice. This principle makes it possible to abstract from the characteristics of a particular object, since such characteristics are taken into account by the recommendation algorithms in determining the liking of the preferences of different users.

According to this principle, the explanation should reflect the popularity of each product or service. The quantification gives an opportunity to compare the popularity of different

DOI: https://doi.org/10.30837/IVcsitic2020201455

items, as well as the changes in popularity over time. Therefore, quantitative assessment makes it possible to satisfy the criterion of confidence [2].

According to this principle, an explanation in numerical form g_j of an item i_j can be represented as a total change in the interests of users for that object over the selected period of time:

$$g_j = \sum_{k:\Delta t_k \in T} \Delta_{k,j}, \quad (1)$$

where $\Delta_{k,j}$ - change of interest of users to the item i_j in the interval of time Δt_k; T - the period of time for which explanations are formed.

The essence of the second principle is to iteratively implement the sequence of adjusting explanations as new consumer choice data is used. This sequence contains the following steps.

Step 1. Formation of explanations for received recommendations according to (1).

Step 2: Implement user feedback from explanations.

In this step, the information in the e-commerce system database changes after the user uses the explanations. Such information may include a list of user-viewed pages of an e-commerce site, change in ratings, increase or decrease in sales.

Step 3: Calculate refined explanations for feedback from the recommendation subsystem user.

The difference between this step and step (1) is to change the time period for the explanation T. That is, when clarifying explanations, a "sliding window" is used:

$$T_{i+1} = T_i - \Delta t_1 + \Delta t_{K+1}, \quad (2)$$

where T_i, T_{i+1} are variants of the periods T of time for which explanations on iterations i, $i+1$ are determined; Δt_1 - the first time interval in the period T_i; Δt_{K+1} - the last time interval in the period T_{i+1}.

According to expression (2), at each iteration the time period for constructing explanations is shifted by an interval Δt_{K+1} on a time scale.

For all time intervals, the following condition is true:

$$\left(\forall k \forall m, k \neq m,\right) \left|\Delta t_k\right| = \left|\Delta t_m\right|, \quad (3)$$

where $\Delta t_k, \Delta t_m$ are two arbitrary intervals within a time period T.

Steps 2 and 3 are repeated as new information is received from users.

The second principle makes it possible to satisfy the Scrutability criteria of the first group and the Persuasiveness criteria of the second group. The Scrutability criterion is aimed at assessing the change in user interests based on the explanations received. To determine such an estimate, it is necessary to compare the list of goods and services received by the user before and after clarification.

The implicit feedback principle eliminates the intentional influence of the user on the explanations received. When making recommendations, they usually use either explicit or implicit feedback.

Explicit feedback is realized through user-rated items. However, such ratings can be faked in the case of shilling attacks. Therefore, using explicit feedback can lead to incorrect explanations.

Implicit feedback comes from moving a user through the pages of an e-commerce site and through a sales log. The first variant of implicit feedback reflects the potential interests of the user. Registration of this information requires the use of appropriate e-commerce site software. It should also be noted that such information is not always reliable, as the buyer may consider alternative purchases, be interested in the characteristics of the goods and services, etc. On the other hand, the interest of the user in the purchase of goods and services is confirmed by his expenses. That is, the latest information is relevant to the interests of the user. This indicates the importance of using the implicit feedback principle. The feedback is represented by the number of sales of items for which an explanation is being formed.

According to this principle, the formation in the explanations (1) uses the difference in the number of sales of items directly for a certain time interval, or for a pair of intervals within one time period.

III. CONCLUSIONS

The principles of explanation are suggested taking into account changes in requirements and interests of users. The proposed principles include the use of quantitative explanation of a recommended product or service, an iterative refinement of the explanation as new user choice information emerges, and the use of implicit feedback to construct explanations. Implicit feedback is information about sales of goods and services within a defined period of time, broken down by intervals of the same length over time.

The proposed principles make it possible to form an explanation based on objective data about changes in sales of goods or services. The objectivity of this data is confirmed by the costs of consumers.

REFERENCES

[1] Aggarwal C. (2017). Recommender Systems: The Textbook, New York: Springer. 498 p.

[2] Tintarev N., Masthoff J. (2007). A survey of explanations in recommender systems, in IEEE 23rd International Conference on Data Engineering Workshop, 801– 810.

[3] Chalyi S., Leshchynskyi V., Leshchynska I. (2019). Method of forming recommendations using temporal constraints in a situation of cyclic cold start of the recommender system. EUREKA: Physics and Engineering, 4, 34-40 DOI:10.21303/2461-4262.2019.00952.

[4] Chala O., Novikova L., Chernyshova L. (2019). Method for detecting shilling attacks in e-commerce systems using weighted temporal rules. EUREKA: Physics and Engineering. Vol. 5, 29-36. DOI: 10.21303/2461-4262.2019.00983

[5] Tintarev N., Masthoff J. (2012) Evaluating the effectiveness of explanations for recommender systems, User Model User-Adap Inter Vol 22, 399– 439.

[6] Modelyuvannya poyasnen shodo rekomendovanogo pereliku ob'yektiv z urahuvannyam temporalnogo aspektu viboru koristuvacha / S. F. Chalyj, V. O. Leshinskij, I. O. Leshinska // Sistemi upravlinnya, navigaciyi ta zv'yazku. - 2019. - Vip. 6. - S. 97-101. - Rezhim dostupu: http://nbuv.gov.ua/UJRN/suntz_2019_6_19

DOI: https://doi.org/10.30837/IVcsitic2020201453

Aspects of Human-Centered Design Application in Control Information Systems

Shekhovtsova Victoriya[1]
Veretelnikov Dmytro[2]
Lebediev Valentyn[3]

[1]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, viktoriia.shekhovtsova@nure.ua*
[2]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, dmytro.veretelnikov@nure.ua*
[3]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, lebedevvalen@gmail.com*

Abstract. *Principles, approaches and methodology of Human-Centered Design, set out in the ISO 9241-210 standard, give recommendations to developers according to the planning and implementation of information systems with interactive components. Analysis of the proposed rules and actions revealed the missing aspects, which, according to the authors, are essential for minimizing the influence of the human factor in information management systems.*

Keywords: *Human-Centered Design, human factor, design principles, usability.*

I. Introduction and Problem Statement

In the "man-technology-environment" system, the weak link is a man. His qualification, experience, ability and willingness to quickly adapt to changing technical and technological innovations and environmental factors do not fully guarantee the ideal result in the design and operation of both information management systems and other IT products.

For the preventive exclusion of the negative impact of the human factor, the methodology Human-Centered Design (hereinafter - HCD), the Scrum and Waterfall models are used. However, the problem is not solved only C. It is necessary to find out the missing aspects, the consideration of which will allow to reduce to zero the negative consequences of human factor.

II. Problem Solution and Results

ISO standard 9241-210. Planning and Implementation HCD highlights six design principles within Human-Centered Design [1]:

1. Design should be based on an accurate definition of users, their tasks and environment.
2. Users should be involved in design and development.
3. Design should be based on user feedback.
4. The process should be iterative.
5. The design addresses the whole user experience.
6. The team must be multidisciplinary.

The standard clearly distinguishes actions of the developer according to the HCD methodology [2]:

1. Identify required resources and suitable methods.
2. Determining how the above methods will be integrated with other development processes.
3. Identification of responsible.
4. Determination of communication channels and methods for resolving contradictions.
5. The time frames of individual stages of the HCD and their integration into overall development plan should be agreed.

As part of the usage context specification, ISO 9241-210 recommends the following actions: [3]:

1. Identify the main user groups and stakeholders (stakeholders).
2. Define the goals and objectives of the above users and stakeholders.
3. Define the technical, organizational and physical environment.

This allows you to formulate product requirements in the following order:

1. Describe product requirements.
2. Resolve conflicts between different requirements.
3. Verify the quality of the stated requirements. Requirements must be:

- Formulated so that in the future the product can be tested in accordance with these requirements;
- Agreed with all interested parties;
- Holistic;
- Relevant and updated throughout the project's life cycle [4].

At the design stage of interaction, it is recommended:

1. Design user tasks, user-system interactions, as well as the interface.
2. Present in details project decisions.
3. Use user feedback to improve design decisions.
4. Deliver design solutions to those who will be involved in the development and implementation [3].

For a proper assessment of compliance with the requirements:

1. Get updated relevant user information.
2. Get feedback as for design weaknesses and strengths.
3. Establish criteria against which you will compare the current and next versions of the project.

In accordance with the obtained results, it is possible:

- invite future users to pass test of the developed information system to identify inaccuracies, missing elements or erroneous accents of the developer;
- listen to the opinion of competent experts with experience in the development and implementation of such products;
- carry out meticulous monitoring of critical situations, incidents and problematic delays, support calls , etc.

If necessary, you can make changes and repeat some of the stages of testing. But all this costs money and time.

DOI: https://doi.org/10.30837/IVcsitic2020201455

Therefore, sooner or later, the project team will have to stop and present their project to the customer.

Such theoretical approach, outlined in the standard, is abstract in nature and can be considered as a recommendation for action, but often cannot act as a standard of rules.

It should be noted that all principles, approaches and methodologies do not take into account the emotional-valuable aspect of users. Even at the stage of planning the implementation of requirements, it is necessary to anticipate a possible change in both the users themselves and their requirements.

The developer cannot foresee absolutely all the consequences of untimely, incorrect or completely wrong user actions. That is why, it is necessary to deliberately set "control points", to fix the slightest deviations from the logic of the process or fluctuations in the responses, user reactions.

III. CONCLUSIONS

All rules and principles work in conditions of their impeccable implementation. The human factor arises when the established algorithm of actions is not followed. Therefore, developers committed to the Human-Centered Design methodology need to focus on the person, as a source of error, and obviously provide ways to eliminate them.

REFERENCES

[1] ISO 9241-210:2019 Ergonomics of human-system interaction — Part 210: Human-centred design for interactive systems& // https://www.iso.org/ru/standard/77520.html

[2] ГОСТ Р ИСО 9241-210-2016 Эргономика взаимодействия человек-система. Часть 210. Человеко-ориентированное проектирование интерактивных систем http://docs.cntd.ru/document/1200141127

[3] ISO 9241-210. Планирование и внедрение Human-Centered Design Usability https://habr.com/ru/post/ 258635/

[4] Top 4 Principles of Human-Centered Design Nick Babich https://uxplanet.org/top-4-principles-of-human-centered-design-5e02751e65b1

[5] A Human-Centered Design Methodology to Enhance the Usability, Human Factors, and User Experience of Connected Health Systems: A Three-Phase Methodology. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5374275/

[6] A lab of labs:methods and approaches for a human-centered design http://www.publishinglab.nl/wp-content/uploads/2017/11/ALabofLabsWEB.pdf

INFOCOMMUNICATION NETWORKS AND TECHNOLOGIES

DOI: https://doi.org/10.30837/IVcsitic2020201455

Method of Hierarchical QoS-Routing in Software-Defined Networks

Lemeshko Oleksandr,
Yevdokymenko Maryna,
Yeremenko Oleksandra

Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine,
oleksandr.lemeshko.ua@ieee.org,
maryna.yevdokymenko@ieee.org,
oleksandra.yeremenko.ua@ieee.org

Abstract. *In the paper, the method of hierarchical QoS based inert-domain routing in Software-Defined Networks has been presented. The novelty of the method is that the obtained routing solutions have to ensure the normalized Quality of Service under indicators of average transmission rate and end-to-end average packet delay. Numerical research has been conducted with the aim of confirming the workability and effectiveness of the method by providing a normalized QoS under the finite number of iterations that help to decrease the amount of overall service traffic.*

Keywords: *inter-domain routing; hierarchical coordination; Quality of Service; end-to-end delay; SDN.*

I. Introduction and Problem statement

Providing a demanded Quality of Service (QoS) for user requests is the primary purpose of modern networks, including Software-Defined Networks, SD-WAN, and Hybrid SD-WAN [1-5]. At the same time, when solving the tasks of routing and traffic management, there is a problem of increasing the scalability of the obtained solutions [1, 4]. Therefore, the paper proposes a method of hierarchical coordination of inter-domain routing in a software-defined infocommunication network. The novelty of the method is that the routing solutions obtained through it are aimed not only at increasing the network scalability, but also at ensuring the normalized QoS under such indicators as average transmission rate and end-to-end average packet delay.

II. Problem solution and Results

The proposed method is based on the use of decomposition of the flow-based inter-domain routing model under the following conditions and constraints:

- implementation of a single path and multipath routing;
- conditions of flow conservation;
- conditions of the overload prevention of network links;
- conditions of inter-domain interaction, which guarantee the connectivity inter-domain routes.

Additionally, the flow-based model of inter-domain routing has been supplemented by the provision of normalized QoS. In order to formulate in an analytical form the conditions for ensuring the normalized QoS, the means of tensor modeling of networks were used with the geometric space, which were respectively created by coordinate paths – edges (links), interpolar paths and internal node pairs.

Therefore, the problem of inter-domain QoS routing under the proposed method was presented as an optimization using the quadratic optimality criterion, which was solved using the principle of goal coordination [6, 7]. Accordingly, two hierarchical levels solved the tasks that were assigned to them:

- the lower level (the level of SDN domain controllers) was responsible for the calculation of intra-domain routes;
- the upper level (the SDN level of the network controller) was responsible for coordinating the lower level solutions by performing inter-domain interaction conditions to ensure inter-domain connectivity within the gradient procedure.

The coordination of routing solutions was completed when the gradient approached zero.

III. Conclusions

The study of the proposed method of inter-domain QoS routing on a number of numerical examples confirmed its workability and effectiveness in terms of providing a normalized QoS. On the ground that, it was found experimentally that the method converged to the optimal solution for the finite number of iterations. Moreover, for network structure under investigation, the number of iterations of the coordination procedure, with the appropriate gradient search, was not more than three iterations. All the things considered, reducing the number of such iterations will decrease the amount of service traffic in the network between routers and SDN controllers at different levels, as well as minimize the overall time of solving the inter-domain QoS routing task.

References

[1] R. White and E. Banks, Computer Networking Problems and Solutions: An innovative approach to building resilient, modern networks 1st Edition. 1 edition. Addison-Wesley Professional, 2018.

[2] G. Blokdyk, Managed Hybrid WAN SD-WAN The Ultimate Step-By-Step Guide, 5STARCooks, 2018.

[3] P. Goransson, C. Black and T. Culver. Software defined networks: a comprehensive approach. Morgan Kaufmann, 2016.

[4] F.X. Wibowo, M.A. Gregory, K. Ahmed and K.M. Gomez, "Multi-domain software defined networking: research status and challenges," Journal of Network and Computer Applications, Vol. 87, 2017, pp. 32-45.

[5] C. Carthern, W. Wilson, N. Rivera and R. Bedwell, Cisco Networks: Engineers' Handbook of Routing, Switching, and Security with IOS, NX-OS, and ASA. Apress, 2015.

[6] O. Lemeshko, O. Yeremenko and O. Nevzorova, "Hierarchical method of inter-area fast rerouting," Transport and Telecommunication Journal, Vol. 18, Iss. 2, 2017, pp. 155-167.

[7] O.S. Yeremenko, O.V. Lemeshko, O.S. Nevzorova and A.M. Hailan, "Method of hierarchical QoS routing based on network resource reservation," in Proc. 2017 IEEE First Ukraine Conference on electrical and computer engineering (UKRCON), pp. 971-976, 29 May-2 June 2017.

DOI: https://doi.org/10.30837/IVcsitic2020201456

Technology of Load Balancing in Anonymous Network Based on Proxy Nodes Cascade Platform

Tkachov Vitalii
Hunko Mykhailo
Bondarenko Maksym
Artyomov Serhii

Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine,
tkachov@ieee.org,
hunko@ieee.org,
bondarenko@ieee.org

Abstract. *The work is devoted to the development of a technology for balancing network traffic between proxy nodes in a cascade scheme. The technology developed involves substituting proxy nodes in case of restricted node overload. The technology improves the fault-tolerance indicator of anonymous network.*

Keywords: *anonymous network, proxy, traffic balancing, computer engineering.*

I. INTRODUCTION

One of the ways to organize the protection of personal information on the Internet is to use anonymous networks [1]. There are a very large number of anonymous networking technologies. One of such technologies is to use a cascade of proxy servers [1, 2]. A classic example of the given technology is the hybrid anonymous Psiphon network. The specifics of its work is that it uses a unique web address, login and password to connect to a proxy server without making any changes to the browser settings. However, this procedure can only be performed by proxies since the proxy administrator has documented information about the user's activity. The user can connect to any point on such a network and, according to the network settings, must pass a certain number of proxy nodes, which anonymizes its traffic.

The problem that arises at the stage of organizing a traffic route is the overloading of individual nodes. This most frequently happens when such an anonymous network uses the existing overlay infrastructure with geo-location of the client by its IP address [3] (including the one dynamically reconfigured with high-mobility nodes [5]). The nodes go into denial of service status or the quality of access decreases significantly. Mirroring of requests to other nodes can reduce traffic anonymity.

Thus, there is an urgent task of developing a balancing technology for network traffic in an anonymous network based on the proxy nodes cascade platform by even distribution of requests.

II. PROBLEM SOLUTION AND RESULTS

The developing technology is based on the use of a restricted proxy class. These are the proxies, the properties of which depend on their use. Limited proxies have capabilities similar to the cascading mechanism of executing operations, the members of which do not trust each other. The essence of technology is that requests for overloaded (but functioning) proxy nodes are redirected into the depth of the anonymous network. The proxy nodes that are less loaded become restricted ones for the requests. This technology is fair for an anonymous network where all proxy nodes are equivalent. Thus, when passing through the proxy node that follows after the first one, i.e. the intermediate proxy node, the standard restrictions are applied to the traffic. They are added by approving a new proxy node with the original key. This technology is also fair to anonymous networks that implement only the delegated proxies where cascading authorization uses only the certificates of the original proxy node. Since the intermediate proxy node is explicitly identified in the original proxy node, it also provides such function of the proxy node, allowing it to act as an intermediate node in order to execute the initial proxy node.

Experimental studies of the given technology were carried out on the basis of the "Reconfigured and Mobile Systems Laboratory" at the Department of Electronic Computers, NURE, and showed that the failure rate of the anonymous network on the platform of the proxy nodes cascade decreased by 15%.

III. CONCLUSIONS

The technology of load balancing in the anonymous network built on the platform of proxy cascades has been considered in the work. The balancing scheme is based on the mechanism of request forwarding between nodes. The results show that the strategy of using the restricted proxy nodes with up-to-date information on the node load gives the least delay in determining the node for receiving traffic from a user.

REFERENCES

[1] Ткачов В.М. Дослідження надійності анонімної мережі на основі каскадної технології проксування / В.М. Ткачов, Д.Є. Мітін, В.С. Волотка // *Дев'ята міжнародна науково-технічна конференція «Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління»*. – Баку-Харків-Жиліна. – 11-12 квітня 2019 р. – С. 40.

[2] Zhang Y., Li J., Chen X., & Li H. Anonymous attribute-based proxy re-encryption for access control in cloud computing. *Security and Communication Networks*, 9(14), pp. 2397-2411.

[3] Tkachov V., Bondarenko M., Ulyanov O. and Reznichenko O. Overlay Network Infrastructure for Remote Control of Radio Astronomy Observatory, *2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT)*, Kyiv, Ukraine, 2019, pp. 161-165.

[4] Churyumov G. Method for Ensuring Survivability of Flying Ad-hoc Network Based on Structural and Functional Reconfiguration / Genadiy Churyumov, Vitalii Tkachov, Volodymyr Tokariev, Vladyslav Diachenko // *Selected Papers of the XVIII International Scientific and Practical Conference "Information Technologies and Security" (ITS 2018)* / Kyiv, Ukraine, November 27, 2018. – Pp. 64-76.

DOI: https://doi.org/10.30837/IVcsitic2020201463

Fast ReRouting Flow-based Model with Implementation of Path Protection

Yeremenko Oleksandra,
Yevdokymenko Maryna,
Sleiman Batoul,
Omowumi Stephen Olayinka

Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine
oleksandra.yeremenko.ua@ieee.org,
maryna.yevdokymenko@ieee.org,
sleimanbatoul@hotmail.com,
iamengineerstephen@gmail.com

Abstract. *In this paper, the fast rerouting model with the implementation of the path protection scheme in the infocommunication network is investigated. Within the proposed Fast ReRoute model with the path protection schemes, the problem of calculating the set of primary and backup disjoint paths was solved. The advantage of the improved model is the possibility of implementing protection schemes 1:1, 1:2, ..., 1:n without introducing an additional set of routing variables. This results in reducing the dimension of the optimization problem to be solved and the computational complexity of its implementation. The optimality criterion of routing solutions contributes to the formation of primary and backup disjoint paths with the maximum bandwidth. Additionally, the path with the highest bandwidth will correspond to the primary path, while the rest of the paths will be used as a backup in decreasing order of their bandwidth.*

Keywords: *Fast ReRouting; path protection; disjoint paths; bandwidth; optimization.*

I. INTRODUCTION

As is known, while ensuring the fault tolerance of the infocommunication network (ICN) at the network level, the key role is given to Fast ReRoute (FRR) protocol solutions [1, 2]. Thus, for the transmission of packet flows the primary and backup routes are calculated with the protection of the Quality of Service (QoS) along them by such QoS indicators as bandwidth, average delay and the probability of packet loss [3, 4]. In addition, the implementation of FRR also raises the problem of calculating the set of disjoint paths [5, 6]. This formulation of the problem meets the requirements of increasing the fault tolerance of routing solutions, especially when the protection of paths and their bandwidth is required. In this regard, the task of development of the FRR model with the implementation of a path protection scheme and bandwidth is relevant. In addition, the proposed model should provide scalability of the obtained solutions and low computational complexity of its further protocol implementation.

II. FAST REROUTING FLOW-BASED MODEL WITH IMPLEMENTATION OF PATH PROTECTION

The paper proposes the FRR flow-based model with the implementation of the path and its bandwidth protection presented by additional conditions. The introduction of these conditions allows reducing the solution of the technological FRR task to the solution of the optimization problem of mixed integer linear programming with a modified optimality criterion that is introduced for inclusion in the calculated routes of links with high bandwidth. The result of solving the formulated optimization problem is the calculation of the set of disjoint routes. Of this set, the route with high bandwidth will correspond to the primary path, while other routes will be used as backup routes in decreasing order of their bandwidth. Thus, each of the calculated routes will have the required bandwidth.

The advantages of the proposed model include the fact that the implementation of the 1:*n* path protection scheme does not lead to a proportional increase in the dimension of the optimization problem. The optimality criterion used is aimed at the fact that the set of calculated paths contains routes that not only meet the bandwidth requirements but also include the most productive communication links. The linearity of the proposed flow-based FRR model and the reduction of the number of routing variables to be calculated helped to decrease the complexity of its computational implementation during the organization of fast routing on the network.

III. CONCLUSIONS

In the course of the study, a comparison of the routing solutions that were obtained using the FRR model with the optimality criteria for different network structures and redundancy schemes – 1:2 and 1:3 has been conducted. The prospect of further research in this area is primarily concerned with the support of multipath routing strategies, as well as the implementation of schemes to protect QoS indicators (bandwidth, average delay, jitter, packet loss probabilities), and Quality of Experience (QoE) indicators, such as rating and multimedia quality.

REFERENCES

[1] J. Rak, Resilient Routing in Communication Networks. 1st edition, Springer, 2015.

[2] D. Tipper, “Resilient network design: challenges and future directions,” in Telecommunication Systems, vol. 56, iss. 1, 2014, pp. 5-16.

[3] O. Lemeshko, M. Yevdokymenko and O. Yeremenko, “Model of data traffic QoS fast rerouting in infocommunication networks,” Innovative Technologies and Scientific Solutions for Industries, Vol. 3, Iss. 9, pp. 127-134.

[4] L. Guo, “Efficient approximation algorithms for computing k disjoint constrained shortest paths,” Journal of Combinatorial Optimization, Vol. 32, Iss. 1, 2016, pp. 144–158.

[5] O. Lemeshko, O. Yeremenko, M. Yevdokymenko, B. Sleiman, A.M. Hailan and A. Mersni, “Computation Method of Disjoint Paths under Maximum Bandwidth Criterion”, in Proc. 3rd IEEE International Conference Advanced Information and Communication Technologies (AICT), 2019, pp. 161–164.

[6] P. Cruz, T. Gomes and D. Medhi, “A Heuristic for Widest Edge-disjoint Path Pair Lexicographic Optimization,” in Proc. 2014 6th International Workshop on Reliable Networks Design and Modeling, 2014, pp.

DOI: https://doi.org/10.30837/IVcsitic2020201461

Optimization Method of Object Packaging in Planning of Mobile Communication Systems Femtocells

Sielivanov Kostiantyn[1],
Al-Vandavi Saif Ahmed Iskandar[2]
Moskalets Mykola[3]

[1]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, sunright@yandex.ua*
[2]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, d_ts@nure.ua*
[2]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, mykola.moskalets@nure.ua*

Abstract. *The problem of placing access points of femtocells in the service area of the mobile base station is considered. A method of optimizing the spatial deployment of femtocells using packaging methods is proposed. Based on the method of joining the single femtocell access points, an algorithm for finding and removing potential nested containers has been built. The proposed method of optimizing the spatial placing of femtocells allows to reduce the time of finding the point of installation in order.*

Keywords: *femtocell, object packaging, planning, access point, container.*

I. INTRODUCTION

When placing access points for femtocells, different situations arise due to the need to improve the quality of service for subscribers. There are different methods for spatial placement of access points of femtocells for cases of facilitating access of subscribers at the borders of the service areas belonging to a base station (BS) of the mobile network (Fig. 1).

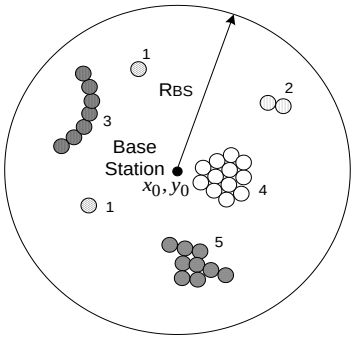


Figure 1. An example of placing femtocells in the BS service area with the coordinates $\{x_0, y_0\}$ and radius R_{BS}

Fig. 1 shows: 1 – single placing; 2 – a group of two femtocells; 3 – linear placing of femtocells; 4 – a compact group; 5 – a complex structure.

As part of the solution to the problem of constructing a network planning technique using femtocells, currently there is no common model for predicting signal propagation, especially when implementing femtocells in buildings. Thus, there is a problem of placing BS access points of femtocells in the service area, both single objects and objects located in a line on the plane or in the structure of the BS functioning area (Fig. 1).

II. PROBLEM SOLUTION AND RESULTS

When planning service areas on the plane, their structure is represented as circles or hexagonal cells. In 3-dimensional space, the area is represented by a circle or a sphere. If we imagine this volume or plane as a container, then there arises a task regarding packaging of objects (femtocells) – axially symmetrical figures of this container [1]. There are a large number of approximate methods of packaging containers with objects of various configurations: genetic algorithms for optimizing packaging of rectangular objects; sequential, i.e. single placing of circles of different radii; methods of packaging cylinders based on Stoyan *phi* -functions; geometric combinatorics, algebraic methods, etc.

Therefore, the choice of a method is determined by the context of the problem being solved. Among the solutions to such problems, the most appropriate method is a single connection based on the logical choice, which allows to increase the capabilities of the network and is relatively simple.

Based on the selected method of single attachment of objects using logical selection and analysis of the remaining free space of the i th container, an algorithm for searching and deleting of nested containers has been constructed. The proposed method of optimizing the spatial placing of femtocells allows to reduce the search time of the installation point by an order of magnitude.

REFERENCES

[1] Moskalets N.V. Ispol'zovanie metoda optimizacii upakovki ob`ektov v zadachah planirovanija femtosot mobil'nyh sistem svjazi. Naukove periodichne vidannja “Cistemi upravlinnja, navigaciï ta zv’jazku”. 2017. №2(42). S.185–187.

[2] Popovskij, V. Control and adaptation in telecommunication system: Mathematical foundations [Text] / V. Popovskij , A. Barkalov, L. Titarenko. Tom 94. Springer Science & Business Media.2011.P.173.

[3] Zaruba, D.V., Ispol'zovanie metodov jevoljucionnoj optimizacii dlja reshenija zadach trehmernoj upakovki [Tekst] / D.Ju. Zaporozhec, Ju.A. Kravchenko // Informatka, vychislitel'naja tehnika i inzhenernoe obrazovanie. 2012. № 2 (9).

[4] Kovalenko, A. A. Upakovka krugovyh cilindrov v cilindricheskij kontejner s uchetom special'nyh ogranichenij povedenija sistemy [Tekst] / A.A. Kovalenko, A. V. Pankratov, T. E. Romanova, P. I. Stecjuk // Zhurnal obchisljuval'noï ta prikladnoï matematiki. 2013. № 1 (111). S.126–134.

[5] Chekanin V.A., A.V. Chekanin. Modeli konstruirovanija ortogonal'noj upakovki ob`ektov [Tekst] / V.A.Chekanin, A.V. Chekanin // Informacionnye tehnologii i vychislitel'nye sistemy. №2. 2014. S.37-45.

DOI: https://doi.org/10.30837/IVcsitic2020201463

Analysis of Innovation in the Field of Data Transfer on Example of Segment Routing

Shloma Oleksandr[1]
Volotka Vadym[2]

[1]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, oleksandr.shloma@nure.ua
[2]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, vadym.volotka@nure.ua

Abstract. *Infocommunications of one of the most important and irreplaceable areas of the modern world. It is difficult to imagine a modern society without the Internet, communications, television. Each discovery in the field of infocommunications has a huge impact on humanity.*

Keywords: *Communications, protocols, data, MPLS, SR, network.*

I. Importance of Technology Development

Nowadays, the speed of technology development is many times greater than in the last century, and not surprisingly, this pace is increasing every year. However, not all spheres are developing at the same speed, which creates unfavorable conditions for the growth of other sectors. For example is the information industry, namely info-communications.

We all use mobile phones, personal computers and other modern technological devices. What do all these devices have in common? And what they have in common is that for a full-fledged functionality they need a network connection, and the actual data exchange. Most communication and switching protocols were developed over 20 years ago and are still in use. Undoubtedly, these communication protocols are outdated and can no longer cope with the required amount of data transfer. As a solution for this problem, was developed a segmented routing (SR) technology, which we will consider in more detail.

II. About Segment Routing

Let's consider segment routing technology in more detail. The concept of Segment Routing itself was developed by the SPRING working group as part of the IETF in 2016 [1]. In the data transmission of modern networks, a label system is used, the so-called programmable path, when the communication protocol does not need to look inside the packet, but just read the label and send the data. This technology has been around for 20 years and over the years it has proven to be effective. This technology is called MPLS (MultiProtocol Label Switching) [2]. It allows you to quickly and easily organize data transfer. Whether it is a large corporate network or a telecom operator. SR is an addition and optimization for MPLS and IPv6. Routing is defined by the sender and the communication node sends the data packet using transmission instructions called segments. But for the distribution of segments, two protocols are required:

1) LDP (Label Distribution Protocol) - responsible for the distribution of labels [3];
2) RSVP (Resource ReSerVation Protocol) - responsible for the reservation of network resources. [4]

These two protocols are control protocols that increase the load on the physical part of the routing and they add some complexity. They must interact with the IGP (Interior Gateway Protocol) [5] and, if somewhere here is a mistake, they can completely reset the all data. The IGP is responsible for transmitting route information.

The SR developers asked themselves to abandon of LDP and RSVP, because if we need identifiers of routers and their interfaces for data transfer, we can use IGP directly with OSPF (Open Shortest Path First). In OSPF protocols contain all information that we need about network connections, which can be supplemented. OSPF is a dynamic routing protocol that searches for the shortest path for data transfer. Transport labels will be directly distributed through the IGP, bypassing the LDP. Thus, some steps in packet processing are skipped, and as a result - performance increases.

III. Results

SR without the extra efforts and problems can complement MPLS without changing the forwarding levels. Then the segments will be transmitted as MPLS tags, and the list of segments as a stack of tags. SR can also be used in IPv6 technology. The so-called new type of SR header (Segment Routing Header) is used. In it, the segment is converted to an IPv6 address, and the list of segments is encoded into a list of IPv6 addresses in the routing header. In this case, the active segment is indicated by the recipient address in a new header.

References

[1] RFC 8402 Segment Routing Architecture [Electronic resource] – Resource access mode: https://www.protocols.ru/WP/rfc8402/.
[2] Segment Routing [Electronic resource] – Resource access mode: http://internetinside.ru/segmentnaya-marshrutizaciya/ /.
[3] LDP protocol [Electronic resource] – Resource access mode: http://iptcp.net/protokol-ldp.html
[4] Reservation protocols [Electronic resource] – Resource access mode: https://www.opennet.ru/docs/RUS/inet_book/4/44/rsv_4496.html
[5] Inerir Gateway Protocol [Electronic source[- Resource access mode: https://searchsecurity.techtarget.com/definition/IG

CONTENT

Scientific publication

«COMPUTER AND INFORMATION SYSTEMS AND TECHNOLOGIES»

Responsible for the release: RUBAN Igor, KOVALENKO Andriy, MARTOVYTSKYI Vitalii.

Computer layout: KOVALENKO Andriy, MARTOVYTSKYI Vitalii

Collection materials are published in the author's version without editing

Approved by the Scientific and Technical Council of Kharkiv National University of Radio Electronics № 6/2 17.04.2020

Format 60x84/8. Paper offset. Garniture of TimeNew.
Cond. print. p. 10,46. Edition 100 copies. Order. № 0505/3-20.

LIMITED LIABILITY COMPANI DISA PLUS Publishing House.
Certificate of the subject of publishing: series DK № 4047 dated 15.04.2011.
Ukraine, 61111, Kharkiv region, Kharkiv, str. Saltovskoye Highway, 154.
e-mail:disadruk@gmail.com

Printed from original layout in Private owned enterprise FLP Petrov V. V.
State register of legal entities and physical persons-businessmen.
Record № 24800000000106167 from 08.01.2009.
Ukraine, 61144, Kharkov, str. Gvardeitzev Shironinzev, 79v, ap. 137.
tel. (057) 78-17-137. e-mail:bookfabrik@mail.ua