UDC 621.39, 004.7

EFFICIENCY ESTIMATION OF COMPUTING GRIDS WITH VARIOUS TRAFFIC TYPES

Shmeleva T.R.

O.S. Popov Odessa national academy of telecommunications,
1 Kuznechna St., Odessa, 65029, Ukraine.
tishtri@rambler.ru

ОЦЕНКА ЭФФЕКТИВНОСТИ ВЫЧИСЛИТЕЛЬНЫХ РЕШЕТОК ПРИ РАЗЛИЧНЫХ ВИДАХ ТРАФИКА

Шмелёва Т.Р.

Одесская национальная академия связи им. А.С. Попова,
65029, Украина, г. Одесса, ул. Кузнечная,1.
tishtri@rambler.ru

ОЦІНКА ЕФЕКТИВНОСТІ ОБЧИСЛЮВАЛЬНИХ ҐРАТОК ЗА РІЗНИХ ВИДІВ ТРАФІКА

Шмельова Т.Р

Одеська національна академія зв'язку ім. О.С. Попова,
65029, Україна, м. Одеса, вул. Кузнечна,1.
tishtri@rambler.ru

Abstract. For the efficiency evaluation of computing grids with different types of traffic, reenterable colored Petri nets are suggested. The principles of constructing models in the form of reenterable colored Petri nets are presented. The advantages of the proposed type of constructing models are shown on an example of a rectangular computing grid with an arbitrary size. The number of vertices for different types of models is estimated. The behavior of the real-size computing grid model is studied for various traffic intensities and distribution functions: Poisson, normal, and Rayleigh. The results of estimating the average packet delivery time and the performance are given under the workload conditions. The adequacy of the constructed reenterable models of computing grids to the models of direct mapping is confirmed. The efficiency of computing grids with conditions of workload and malicious traffic is investigated; the results of computing experiments with different kinds of malicious traffic are confirmed.

Key words: computing grid, efficiency estimation, reenterable colored Petri net, traffic attack, deadlock.

Аннотация. Для оценки эффективности вычислительных решеток при различных видах трафика предложено использовать реентерабельные раскрашенные сети Петри. Представлены принципы построения моделей в форме реентерабельных раскрашенных сетей Петри. Показаны преимущества предложенного вида построения моделей на примере прямоугольной вычислительной решетки произвольного размера. Оценено количество вершин для разных видов моделей. Исследовано поведение модели вычислительной решетки реального размера при различных интенсивностях и законах распределения трафика: Пуассона, нормальный и Рэлея. Приведены результаты оценки среднего времени доставки пакета и производительности решетки в условиях рабочей нагрузки. Подтверждена адекватность построенных реентерабельных моделей вычислительных решеток моделям прямого отображения. Исследована эффективность вычислительных решеток в условиях рабочей нагрузки и злонамеренного трафика, подтверждены результаты вычислительных экспериментов при разных видах злонамеренного трафика.

Ключевые слова: вычислительная решетка, оценка эффективности, реентерабельная раскрашенная сеть Петри, злонамеренный трафик, тупик.

Анотація. Для оцінки ефективності обчислювальних ґраток за різних видів трафіка запропоновано використовувати реєнтерабельні розфарбовані сітки Петрі. Надано принципи побудови моделей у формі реєнтерабельних розфарбованих сіток Петрі. Показано переваги запропонованого виду побудови моделей на прикладі прямокутної обчислювальної ґратки довільного розміру. Оцінено кількість вершин для різних видів моделей. Досліджено поведінку моделі обчислювальної ґратки реального розміру за різних інтенсивностей і законів розподілу трафіка: Пуассона, нормальний і Релея. Надано результати оцінки середнього часу доставки пакета і продуктивності ґраток в умовах робочого навантаження. Підтверджено адекватність побудованих реєнтерабельних моделей обчислювальних ґраток моделям прямого відображення. Досліджено ефективність обчислювальних ґраток в умовах робочого навантаження і зловмисного трафіка, підтверджені результати обчислювальних експериментів за різних видів зловмисного трафіка.

Ключові слова: обчислювальна ґратка, оцінка ефективності, реєнтерабельна розфарбована сітка Петрі, зловмисний трафік, тупик.

Computing grids [1, 2] and cloud technologies [3] are an integral part of modern telecommunications networks in all their diversity. Investigation of the properties of these systems requires the construction of complex models with the interaction of an unlimited number of devices and their various combinations [4].

The traditional method of constructing models is a direct mapping [5, 6] which requires a reconfiguration of the model for each new topological scheme of the network and allows to investigate grids of a relatively small size [7, 9]. Then the actual problem arises for constructing models [8] of computational grids of arbitrary size having the model structure completely independent of the network topology.

The classical Petri nets generalized on infinite sets of vertices is an algorithmically universal system [4, 10]. However, the direct application of infinite nets to estimate the timed and probabilistic characteristics of the simulated systems is difficult; the main application area of such models is the verification of the systems behavior and protocols by analytical methods.

The aim of this paper is the efficiency estimation of computing grids represented in the form of reenterable colored Petri nets with various types of traffic. The reenterable colored Petri nets are used for constructing the grid model with an arbitrary size, estimation of the QoS parameters and the performance of grids as well as to identify the possibility of the computing grid blocking and deadlocks which influences the network security.

Basic principles of models construction of telecommunication networks and computing grids via reenterable colored Petri nets. A colored Petri net [5] is a universal algorithmic system and a convenient tool [9] for modeling telecommunication networks and computing grids [4, 6]. There are the following advantages of a colored Petri net: convenience of the graphical representation, conciseness of constructs of the functional ML programming language, the possibility of combining analytical and simulation methods for model research. The traditional method of constructing models is the direct mapping of the network topology in the structural elements of the colored Petri net. The disadvantage of this method is the necessity to reconfigure the model for each new topological scheme of the network.

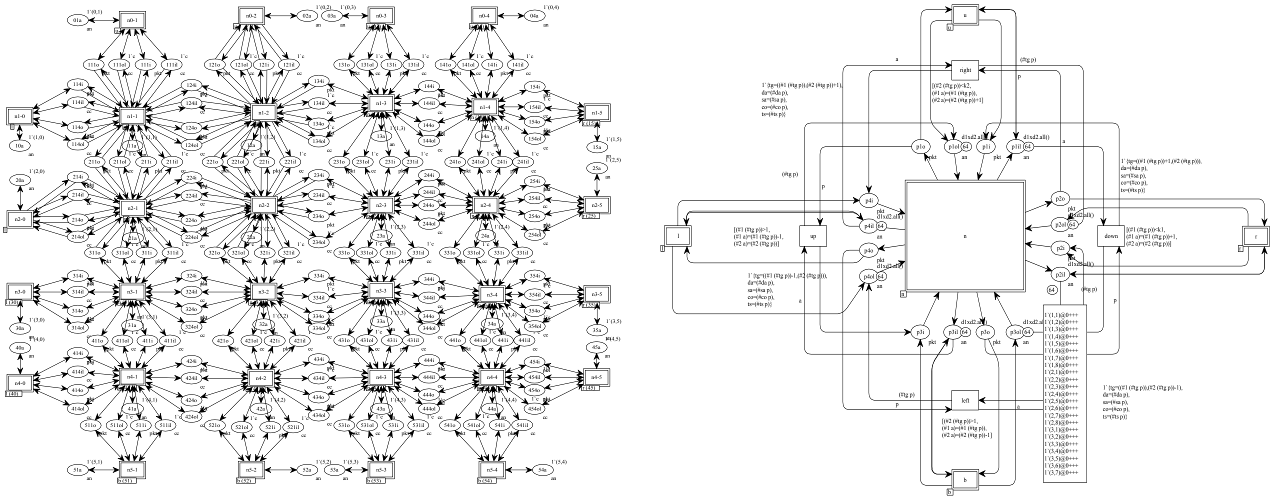
For models construction and researching the computing grids with an arbitrary size, we propose to use the reenterable colored Petri nets. Reenterability involves combining same-function model elements with different indices (tags) into one element which as a result significantly reduces the size of the model and increases the efficiency of its use. There is the following description of the basic principles of constructing reenterable models:

1. For dynamic objects of a model and its structure, a set of tags is formed. In a grid model, dynamic objects are packets generated by terminal nodes.
2. Procedures for switching tags are developed depending on the structure and rules of the grid composition.
3. The grid topology is encoded and represented by the set of parameters in the form of the place marking of a colored Petri net.
4. The basic elements of grid model are adapted in accordance to 1 … 3. The basic elements of grid models are the communication node (CN), the terminal node (TN), and traffic gun.

The principles of reenterable models construction use the method of models composition [6, 10] and the basics of colored Petri nets theory [4, 5]. Applying the principles of reenterable models construction for telecommunication systems and grids, we will consider using the model of a rectangular communication grid with an arbitrary size, a communication device of grid implements the store-and-forward (SAF) technology of packet switching with a buffering.

There are two main methods of packet switching which dominate in telecommunication networks and systems. The first is store-and-forward [7], and the second is without buffering or cut-through [8]. Hybrid switches are also applied in networks; they can be automatically reversed from the cut-through mode to the SAF mode and vice versa. Switching between the modes is based on the determination of performance and the integrity of the package. Most of the modern switches support concurrently different packet rates but SAF technology is traditional for most networks.

Reenterable model of computing grids. Let's give a case study considering the principles of reenterable models construction on an example of the rectangular communication grid model [8] with a communication device that implements store-and-forward packet switching [7]. All models were constructed in the environment of CPN Tools modeling system [9]. Fig. 1 shows the models of computing grids; Fig. 1,*a* – direct mapping of 4 × 4 grid; Fig. 1,*b* – reenterable model of *n* × *n* grid.



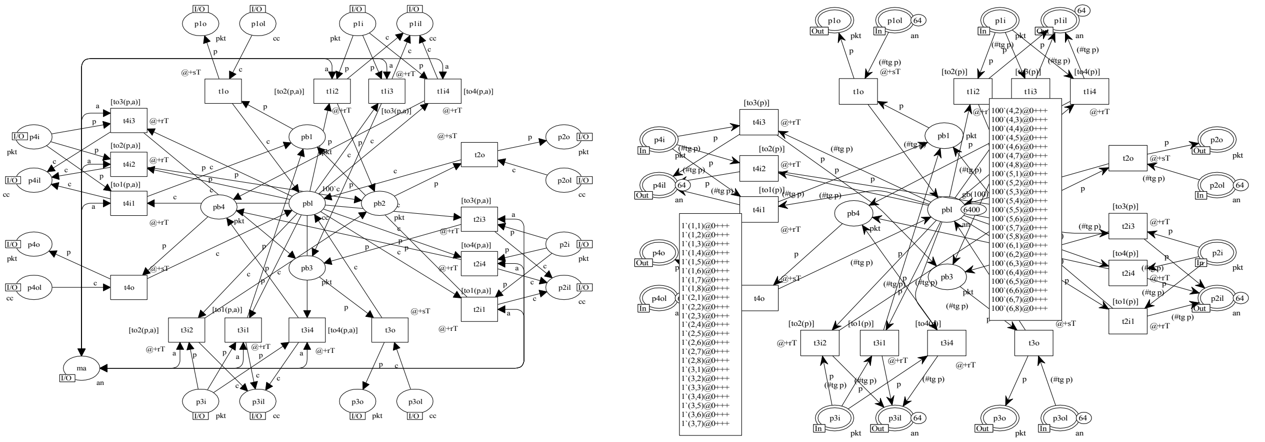
a) *b*)

Figure 1 – Model of computing grids:
a) direct mapping of 4 × 4 grid; *b*) reenterable model of *n* × *n* grid

The models of the communication nodes are represented by a single submodel of the transition "n" that describes all nodes of grid with an arbitrary size, and by 16 combined places located on the sides of the transition which describe all the port of all the communication nodes. The models of terminal nodes are represented by four submodels; they are the transitions with the names "u, b, l, r" (named after: upper, bottom, left, right). The grid topology is encoded as a marking of the places which describe all ports of communication nodes. For example the marking of *p4il* place describes buffer limits of all forth ports of communication nodes 1\`(1,1), 1\`(1,2), …, 1\`(*i*, *j*), …, 1\`(*n*, *n*), where (*i*, *j*) are port indexes.

Reenterable model of communication nodes. Fig. 2 shows the models of communication nodes; Fig. 2,*a* – direct mapping; Fig. 2,*b* – reenterable model. The grid topology is marking of the places which describe all ports of communication nodes.

The number of communication nodes for a grid with size $k1 \times k2$ is equal to $k1 * k2$. The grid model with size $k1 \times k2$ is optimized by replacing all models of grid communication nodes by one model which contains a marking equal to the grid size in the corresponding places. The internal buffer size of the node is calculated as the product of the number of grid nodes by the size of one buffer.



a) *b*)

Figure 2 – Model of CN with SAF: *a*) direct mapping; *b*) reenterable model

In the grid model the packet switching decision is implemented via the predicates *toX(p,a)* which allow packet forwarding to port *X*. For direct mapping and reenterable models these predicates are different, because of the tags used in the reenterable model. Fig. 3 shows the full declaration of predicates *toX(p,a)*.

```
fun to1(p:pkt,a:an)=v1(p,a) andalso ((not (db1(p) andalso cb1(a))) orelse (db1(p) andalso cb1(a)
andalso nb1(p,a)))

fun to1(p:pkt)=v1(p,(#tg p)) andalso ((not (db1(p) andalso cb1((#tg p)))) orelse (db1(p) andalso
cb1((#tg p)) andalso nb1(p,(#tg p))))
```

Figure 3 – Description of function *to1()*

Transformation of the terminal node model. For performance and QoS parameters evaluation of grids, the terminal nodes (TNs) models are added to the edge ports. A TN generates packets according to the selected random distribution function having the sender and receiver addresses for the following switching. The CPN Tools modeling system [5, 9] contains a wide range of known distribution functions for describing the user random traffic. Direct mapping of TN models are studied in [6, 7], reenterable models of TNs are studied in [8].

The models of measuring fragments [4] for the calculation of grid characteristics can be represented by individual reenterable submodels or added as Petri net elements to the model of terminal and communication nodes as well as to the main page of the grid model.

Table 1 shows a number of vertices in the computing grid models with different sizes and types.

Table 1 – Number of vertices in a computing grid models

Type of a model	Grid model	Number of CN models	Number of CN vertices	Number of TN models	Number of TN vertices	Total
Direct mapping 2×2	72	4	148	8	160	360
Direct mapping 4×4	224	16	592	12	240	1056
Direct mapping 8×8	648	64	2368	32	640	3656
Reenterable $n \times n$	25	1	36	4	80	141

A reenterable model of *n* × *n* computing grid consists of the constant number of vertices for grid of any size. The models which were constructed by direct mapping consist of the greater number of vertices than the reenterable model: the 2 × 2 grid is greater in 2,5 times, 4 × 4 grid is greater in 7,5 times, 8 × 8 grid is greater in 26 times. Thus, the reenterable model brings efficiency to the modern networks and computing grids design.

Efficiency estimation of computing grid model under workload with various traffic types. The reenterable model allows to research a grid with any size *n* × *n*; grid models with sizes 2 × 2 and 8 × 8 were constructed by direct mapping and studied in [6, 7]. For investigation of the grid behavior under workload and estimation of the grid efficiency, we use a closed rectangular grid with size 32 × 32. Random function *Delay()* defines the period of users packet's generation, and describes the incoming users traffic intensity *wl* in the grid. In this research we estimate efficiency of computing grid model when *wl* is described by three random functions: Poisson, Normal, and Rayleigh. The performance of the communication device is a constant and is equal to the time parameter *rT* = 5; the CN internal buffer size is *bs* = 100.

Table 2 shows the results of the computing experiments, the calculations are carried out in model time units (MTU); a number of modeling system steps is *Step* = 1 000 000; * – the grid comes to complete deadlock, there are no permitted transitions. Normal distribution has two parameters; the first is mean, the second is variance.

Table 2 – QoS parameters of 32 × 32 grid

Distribution function	Workload intensity	Time	Average packet delivery time (MTU)	Grid performance (packets/MTU)	Number of sent packets	Number of received packets
Poisson	30,0	2751	301	3,79	11848	10432
Poisson	15,0	1594	377	5,57	13653	8892
Poisson	2,0*	820	330	7,25	21058	5924
Normal	30,0; 1.0	2851	298	3,67	11776	10450
Normal	15,0; 1,0	1695	373	5,26	13696	8908
Normal	1,0; 1,0*	820	332	7,34	21296	6013
Rayleigh	30,0	5382	296	2,03	11392	10873
Rayleigh	15,0	1751	372	12,37	13197	9295
Rayleigh	2,0*	815	330	7,37	21168	6007

Under the low workload when users traffic intensity is *wl* = 30,0, a grid has the state stable mode of model's behavior for any distribution function. Average packet delivery times are approximately equal and grid performances are not greater than twice. For the middle workload with users traffic intensity is *wl* = 15,0, the average packet delivery times are approximately equal too, the grid performance for Rayleigh distribution is better than Poisson and Normal. For these distributions, the grid performances are approximately equal. When *wl* parameter is decreased, the average packet delivery time increases, and the grid comes to the complete deadlock in a small interval of model time. Deadlock types were studied in [6, 10]; grid behavior under workload and users traffic intensity which is described by Poisson distribution function was studied in [7].

Efficiency estimation of computing grid model during traffic attacks. For simulating traffic attacks we use the model of a packet gun [7] which is attached to the grid borders. The intensity of guns and location of their targets are the main parameters for investigation of their influence on the model behavior. We estimate the 8 × 8 computing grid, the intensity of the users traffic is $wl = 30{,}0$ as well as of traffic attacks is $gl = 5{,}0$ and they have a Poisson nature.

Packets which are generated by guns are added to the regular traffic of grid model, and we study their influence on the model behavior. The time until complete deadlock and the percentage of packets fired by guns are the basic characteristics of grid behavior. In this research, the efficiency of computing grid model was estimated by the calculation of two parameters: an average packet delivery time and a grid performance. The most significant results were obtained for the four types of traffic attack [6], shown in Fig. 4, 5.

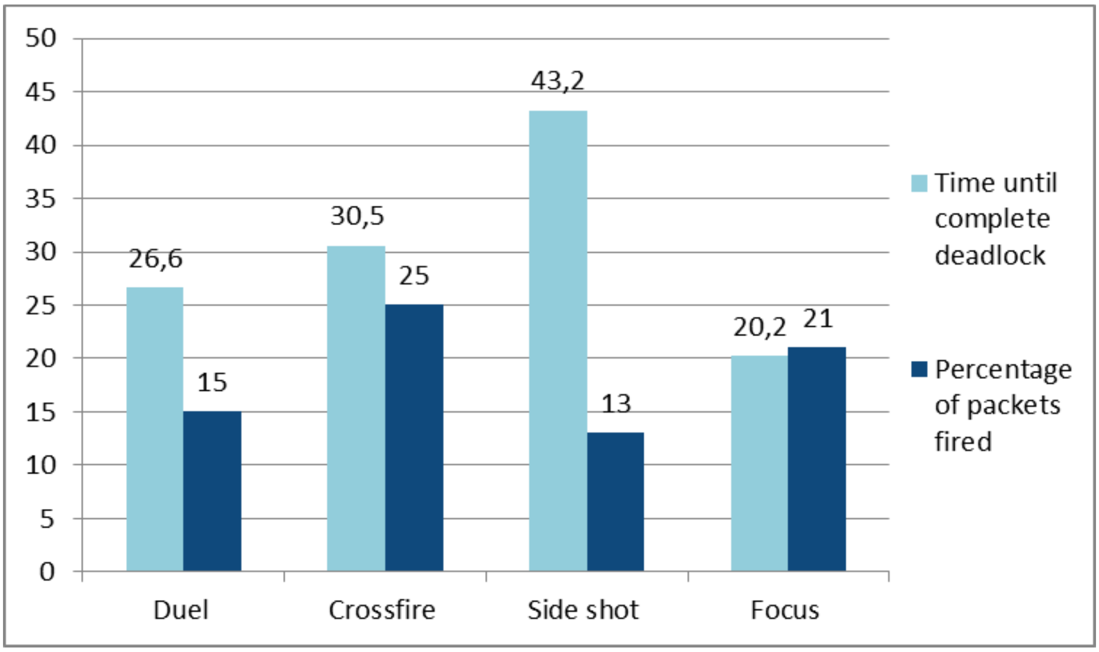
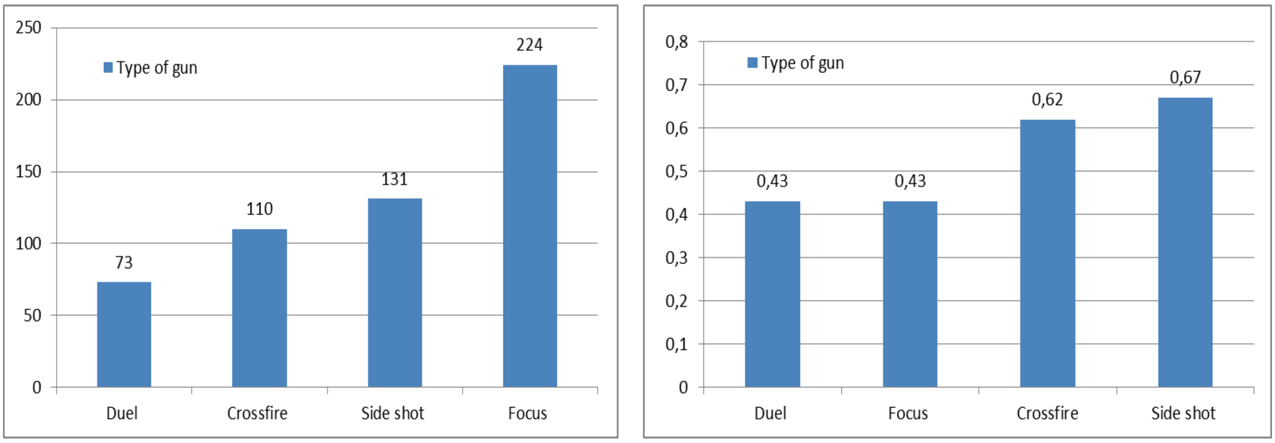


Figure 4 – Comparing traffic attacks

The obtained results for the four types of traffic attack are equal to the results which were illustrated in [6]. Fig. 4 shows that a Side shot attack requires less intensive guns and has maximum time until complete deadlock. Duel attack is more malicious and disguised than others attacks, a Focus is faster in bringing the grid to deadlock, and a Crossfire attack has the worst result in experiment under research conditions.



a) *b*)

Figure 5 – Comparing parameters of grid efficiency:
a) average packet delivery time (MTU); *b*) grid performance (packets/MTU)

Fig. 5 shows that a Focus has maximum value of average packet delivery time and low grid performance, it is more distinct attack. Crossfire and a Side shot attacks provide a positive grid performance and valid value of average packet delivery time, but a Duel attack has relatively better values of QoS.

The reenterable models allow us to investigate the problems of blocking grids under working and malicious traffic for grids with a big (real life) size in feasible time. The behavior of rectangular grid with size 32 × 32 was investigated under the workload; the users traffic intensity is described by random functions: Poisson, Normal, and Rayleigh. For small networks sizes, the results are the same as those obtained with traditional models. Results of comparing traffic attacks' parameters and efficiency of an 8 × 8 computing grid model confirm the advantages of reenterable models.

The reenterable models with encoding of topology and tag switching are a perspective direction for the efficiency estimation and security of modern technologies of telecommunication networks, computing grids and clouds.

REFERENCES:

1. Preve, N.P. (Ed.). Grid Computing: Towards a Global Interconnected Infrastructure. Springer. – 2011. – 312 p.
2. R. Dautov, I. Paraskakis, M. Stannett, Towards a framework for monitoring cloud application platforms as sensor networks, Cluster Computing 17 (4) (2014), P. 1203-1213.
3. Grid and Cloud Computing: Concepts, Methodologies, Tools and Applications, vol. 4. Information Resources Management Association (USA), IGI-Global (2012).
4. Zaitsev D.A. Clans of Petri Nets: Verification of protocols and performance evaluation of networks, LAP LAMBERT Academic Publishing. – 2013. – 292 p.
5. Jensen, K., Kristensen, L.M. Coloured Petri Nets: Modelling and Validation of Concurrent Systems. Springer-Verlag Berlin Heidelberg, Germany. – 2009. – 384 p.
6. D. A. Zaitsev , T. R. Shmeleva, W. Retschitzegger, B. Pröll Security of grid structures under disguised traffic attacks. Cluster Computing.– 2016. – 19(3). – P. 1183–1200.
7. Zaitsev D.A., Shmeleva T.R., Retschitzegger W. and Proll B. Blocking Communication Grid via Ill-Intentioned Traffic, 14th Middle Eastern Simulation & Modelling Multiconference, February 3-5, 2014, Muscat, Oman. – 2014. – P.63-71.
8. Shmeleva T.R. Parametric Colored Petri net model of Computing Grids / T.R. Shmeleva // 69 NT conference ONAT, December 3-5, 2014, Odessa. – 2014. – P. 41-43.
9. Modelling system a CPN Tools http://www.cpntools.org.
10. D. A. Zaitsev, I. D. Zaitsev and T. R. Shmeleva. Infinite Petri Nets: Part 1, Modeling Square Grid Structures. Complex Systems, 26 (2), 2017. – P.157-195.

ЛИТЕРАТУРА:

1. Preve, N.P. (Ed.). Grid Computing: Towards a Global Interconnected Infrastructure. Springer. – 2011. – 312 p.
2. R. Dautov, I. Paraskakis, M. Stannett, Towards a framework for monitoring cloud application platforms as sensor networks, Cluster Computing 17 (4) (2014), P. 1203-1213.
3. Grid and Cloud Computing: Concepts, Methodologies, Tools and Applications, vol. 4. Information Resources Management Association (USA), IGI-Global (2012).
4. Zaitsev D.A. Clans of Petri Nets: Verification of protocols and performance evaluation of networks, LAP LAMBERT Academic Publishing. – 2013. – 292 p.
5. Jensen, K., Kristensen, L.M. Coloured Petri Nets: Modelling and Validation of Concurrent Systems. Springer-Verlag Berlin Heidelberg, Germany. – 2009. – 384 p.
6. D. A. Zaitsev , T. R. Shmeleva, W. Retschitzegger, B. Pröll Security of grid structures under disguised traffic attacks. Cluster Computing.– 2016. – 19(3). – P. 1183–1200.
7. Zaitsev D.A., Shmeleva T.R., Retschitzegger W. and Proll B. Blocking Communication Grid via Ill-Intentioned Traffic, 14th Middle Eastern Simulation & Modelling Multiconference, February 3-5, 2014, Muscat, Oman. – 2014. – P.63-71.
8. Shmeleva T.R. Parametric Colored Petri net model of Computing Grids // 69 НТ конференция ОНАС, декабрь 3-5, 2014, Одесса. – 2014. – С.41-43.
9. Моделирующая система CPN Tools http://www.cpntools.org.
10. D. A. Zaitsev, I. D. Zaitsev and T. R. Shmeleva. Infinite Petri Nets: Part 1, Modeling Square Grid Structures. Complex Systems, 26 (2), 2017. – P.157-195.