МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
Одеський національний політехнічний університет

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Том 2, № 2

Volume 2, No. 2

Одеса – 2012
Odesa – 2012

Інформатика та математичні методи в моделюванні
Науковий журнал
Виходить 4 рази на рік
Заснований Одеським національним політехнічним університетом у 2011 році
Свідоцтво про державну реєстрацію
КВ № 17610 - 6460Р від 04.04.2011р.

Informatics and mathematical methods in simulation
Scientific journal
Published 4 times a year
Founded by Odessa National Polytechnic University in 2011
Certificate of State Registration
КВ № 17610 - 6460P of 04.04.2011

Друкується за рішенням редакційної колегії та Вченої ради Одеського національного політехнічного університету
Оригінал-макет виготовлено редакцією журналу

Адреса редакції: просп. Шевченка, 1, Одеса, 65044, Україна
Телефон: +38 048 734 8506
Web: http://immm.opu.ua E-mail: immm.ukraine@gmail.com
Editorial address: 1 Shevchenko Ave., Odessa, 65044, Ukraine
Tel.: +38 048 734 8506
Web: http://immm.opu.ua E-mail: immm.ukraine@gmail.com

ЗМІСТ / CONTENTS

УДК 004.056.53:530.145

Informatics and Mathematical Methods in Simulation
Vol. 2 (2012), No. 2, pp. 99-112

СУЧАСНІ КВАНТОВІ ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Є.В. Василіу

Одеська національна академія зв'язку ім. О.С. Попова,
вул. Ковальська, 1, Одеса, 65029, Україна; e-mail: vasiliu@te.net.ua

У статті на основі виконаних раніше систематизації та класифікації квантових технологій захисту інформації надано характеристику основних напрямків сучасної квантової криптографії з точки зору використовуваних квантових технологій. Розглянуті основні властивості квантових систем, які використовуються у квантовій криптографії. Наведено короткий опис основних типів квантових протоколів розподілення ключів, виконано детальний аналіз їх переваг та недоліків. Розглянуто поточний стан проблеми практичного використання квантової криптографії в інформаційно-комунікаційних системах, зокрема, дано короткий огляд існуючих комерційних систем квантового розподілення ключів.

Ключові слова: квантова криптографія, кубіт, кудит, властивості квантових систем, квантові протоколи розподілення ключів, комерційні системи квантової криптографії

Вступ

На сьогодні першочерговим чинником, що впливає на складові національної безпеки держави, є ступінь захищеності її інформаційного середовища. Питання інформаційної безпеки набуває актуальності як внаслідок стрімкого розвитку комп'ютерних технологій, так і у контексті різкого збільшення злочинів та інших протиправних дій, спрямованих на порушення конфіденційності, цілісності та достовірності інформації. Основна роль у забезпеченні інформаційної безпеки в сучасних інформаційно-комунікаційних системах (ІКТ) відводиться криптографічним методам захисту інформації.

Останнім часом значний інтерес викликає квантова криптографія, стійкість якої ґрунтується на квантових властивостях окремих фотонів, що слугують носіями інформації в системах квантової криптографії. Теоретичні та експериментальні роботи з квантової криптографії ведуться в багатьох науково-дослідних центрах розвинених країн. За минулі з моменту початку активних досліджень два десятиріччя запропоновано багато квантових криптографічних протоколів, виконано значну кількість лабораторних експериментів з їх практичної реалізації, виконана важлива робота з доведення стійкості запропонованих протоколів до деяких видів атак, а також розроблені перші комерційні системи квантового розподілення ключів.

Таким чином, кількість нових методів та протоколів квантової криптографії з часом невпинно зростає. Проте, автори статей у науковій періодиці розглядають, як правило, деякий конкретний квантовий криптографічний протокол, або декілька протоколів, не проводячи при цьому порівняльного аналізу з іншими протоколами та методами квантової криптографії. Це не дає змоги побачити загальну картину, а також оцінити у повній мірі рівень існуючих досягнень для їх подальшого ефективного використання. Відзначимо, що в першу чергу це відноситься до вітчизняної наукової періодики, де взагалі тематика квантових методів захисту інформації поки ще представлена не такою

і великою кількістю робіт. *Метою даної статті* є загальний огляд та порівняльний аналіз сучасних квантових технологій захисту інформації в ІКТ, а також аналіз переваг та недоліків, перспектив та труднощів їх практичного впровадження.

Загальна класифікація сучасних квантових технологій захисту інформації в ІКТ

Основна ідея квантових методів захисту інформації, яка передається в ІКТ, полягає в тому, що класична інформація (криптографічний ключ або відкритий текст повідомлення) кодується станами квантових систем і передається окремими квантовими частинками. В якості таких квантових частинок у протоколах квантової криптографії використовують фотони, а в якості квантового каналу – оптоволоконні лінії або атмосферу (оптичний бездротовий канал). Згідно з законами квантової фізики, операції над квантовими системами призводять до змін їх станів. Тому зловмисник, який бажає перехопити інформацію, неминуче змінює стани передаваних фотонів, що завжди можуть виявити легітимні користувачі. Їх подальші дії залежать від того, який саме протокол і в яких умовах реалізується.

Таким чином, квантові технології захисту інформації, що передається, дозволяють виявити атаку пасивного перехоплення (підслуховування) в каналі зв'язку, що не завжди можливо при використанні традиційних (класичних) методів. Виявлення такої атаки критично як при розподіленні секретних ключів шифрування, так і при передаванні відкритих текстів. Квантові протоколи розподілення ключів дозволяють не тільки виявити атаку пасивного перехоплення, але й за допомогою постобробки переданої інформації видалити інформацію, яку міг отримати зловмисник, і, таким чином, забезпечити розподілення ключів з безумовною (теоретико-інформаційною) стійкістю. Аналогічно, високий рівень безпеки може бути забезпечений при використанні квантових протоколів прямого безпечного зв'язку, які призначені для безпосереднього, тобто без шифрування, передавання відкритих текстів.

На даний час до складу квантових технологій захисту інформації входять: квантове розподілення ключів [1-6], квантовий прямий безпечний зв'язок [4-10], квантове розділення секрету [11, 12], квантовий потоковий шифр [13, 14], квантовий цифровий підпис [15, 16] та квантова стеганографія [17-19].

На рис. 1 наведена загальна схема класифікації квантових методів захисту інформації за їх призначенням, а також за використовуваними квантовими технологіями [6].

Більшість запропонованих на теперішній час протоколів квантової криптографії використовують дворівневі квантові системи – кубіти (*qubit*), що дозволяє передавати класичну інформацію бітами. Але інформаційну місткість квантових протоколів можна підвищити, використовуючи багаторівневі квантові системи, тобто передаючи класичну інформацію тритами, квартами тощо. Відповідно трирівнева квантова система отримала назву кутриту (*qutrit*), чотирирівнева – кукварту (*ququart*) тощо. В загальному випадку *d*-рівнева квантова система називається кудитом (*qudit*). З технічної точки зору в протоколах квантової криптографії носіями як кубітів, так і багаторівневих квантових систем є фотони, але оперувати з багаторівневими системами дещо складніше, ніж з кубітами. Так чином, протоколи квантової криптографії можна поділити на дві великих групи відносно того, дво- або багаторівневі квантові системи в них використовуються (рис. 1).

З іншого боку, квантові системи, що складаються з двох або більшої кількості квантових частинок, можуть находитися в переплутаних станах, тобто в таких станах між цими частинками існують суто квантові кореляції [1, 2]. Локальні операції над однією з частинок переплутаного стану призводять до зміни всього стану. Це дозволяє кодувати класичну інформацію, діючи на одну з частинок, у той час як друга знаходиться у іншого абонента квантового протоколу (наприклад, пінг-понг протокол [7-9]). Використання властивостей квантових переплутаних станів дозволяє забезпечити висо-

кий рівень безпеки протоколів квантової криптографії, а також підвищити їх ефективність. Таким чином, протоколи квантової криптографії можна також поділити на дві великі групи відносно того, одиночні або переплутані квантові системи в них використовуються (рис. 1).

Квантове розподілення ключів є на даний час найбільш розвиненим напрямом квантових технологій захисту інформації, як з теоретичної, так і з практичної точки зору. На лабораторному обладнанні вже виконано значну кількість експериментів з квантового розподілення ключів, наприклад [2, 20-23]. Існують також комерційні системи, повністю придатні для інтеграції в сучасні інфокомунікаційні мережі (їх характеристики коротко розглянуті далі). З цих причин, далі в цій статті розглянуті тільки протоколи квантового розподілення ключів.

Перерахуємо тепер коротко основні властивості квантових систем, які використовуються в квантовій криптографії [1]:

1) Вимірювання фізичних характеристик квантових систем (спостережуваних).

У результаті процесу вимірювання деякої фізичної величини стан квантової системи змінюється. Це обумовлено впливом на квантовий об’єкт вимірювального приладу, який принципово неможливо зробити як завгодно малим. Чим точніше вимірювання, тим сильніший вплив, що воно здійснює, і лише при вимірюваннях дуже малої точності вплив на об’єкт вимірювання може бути досить слабким.

Крім того, збурювання, яке вноситься взаємодією квантового об’єкта з вимірювальним приладом, може бути передбачено тільки статистично й тому не може бути виключено. Цей факт перебуває в різкому протиріччі із класичною теорією вимірювань, яка базується на припущенні, що взаємодія між об’єктом і приладом, якщо й не може бути зроблена як завгодно малою, то принаймні може бути точно врахованою й, отже, у принципі її можна виключити.

2) Неможливість точного копіювання невідомих квантових станів (теорема про заборону копіювання).

Внаслідок лінійності й унітарності квантової механіки, неможливо створити точну копію невідомого квантового стану. Таким чином, зловмисник не може виготовити точну копію кубітів або кудитів, що передаються комунікаційним каналом, щоб провести вимірювання над копією, а оригінал переслати законному користувачеві каналу, не проводячи над ним вимірювання. Цей факт лежить в основі більшості протоколів квантової криптографії, тому що змушує зловмисника вимірювати передавані кудити, або переплутувати їх зі своїми допоміжними квантовими системами, що призводить до зміни станів цих кудитів. Ці зміни передаваних станів можуть виявити законні користувачі, виконуючи квантові вимірювання й обмінюючись результатами цих вимірювань по звичайному відкритому (але аутентифікованому) каналу зв’язку. Відзначимо, що ймовірність правильно скопіювати довільний стан кубіту, створивши одну його копію, дорівнює 5/6 [1]. Якщо потрібно створити n копій невідомого стану кубіту, то ймовірність правильного копіювання зменшується та при $n \to \infty$ прямує до 2/3 [1].

3) Неортогональні квантові стани неможливо розрізнити.

Квантова система із двома станами – кубіт – може перебувати не тільки в базисних станах $|0\rangle$ та $|1\rangle$ (які відповідають, наприклад, вертикальній та горизонтальній поляризації окремого фотону), але й у стані лінійної суперпозиції

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle, \qquad (1)$$

де α й β – комплексні числа, що задовольняють умові $|\alpha|^2 + |\beta|^2 = 1$. Вимірюючи стан кубіту, ми знайдемо, що кубіт з імовірністю $|\alpha|^2$ несе значення «0», а з імовірністю $|\beta|^2$ – значення «1».

Відзначимо, що суперпозиція квантових станів не має аналога в класичній фізиці.

Внаслідок законів квантової механіки неможливо виконати вимірювання, що дозволило б розрізнити стани $|\Psi_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle$ та $|\Psi_2\rangle = \alpha_2|0\rangle + \beta_2|1\rangle$, крім випадку, коли скалярний добуток $\langle\Psi_1|\Psi_2\rangle = 0$, тобто стани $|\Psi_1\rangle$ й $|\Psi_2\rangle$ ортогональні.

4) Переплутування (квантові кореляції).

Дві або більше квантових системи можуть бути переплутані. Так, пара фотонів у синглетному поляризаційному стані

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_1|1\rangle_2 - |0\rangle_2|1\rangle_1\right), \qquad (2)$$

де індекси позначають номери фотонів, – це приклад максимально переплутаного стану двох кубітів. Такий стан називають парою Ейнштейна–Подольського–Розена (ЕПР-парою).

Якщо вимірювання виконується над одним із двох переплутаних кубітів в стані $|\Psi^-\rangle$ (2), наприклад, в базисі $\{|0\rangle, |1\rangle\}$, який називається «обчислювальним базисом», то результат буде «0» або «1» з однаковою ймовірністю 1/2. Стан другого кубіту антикорельований з першим, тобто якщо перший кубіт в результаті вимірювання перейшов у стан $|0\rangle$, то другий перейде в стан $|1\rangle$ і навпаки. Без проведення вимірювання, однак, жодний із цих двох кубітів не перебуває у визначеному стані. Відзначимо, що переплутування, як і суперпозиція станів, – винятково квантові ефекти, що не мають аналога для об'єктів класичної фізики.

Основні квантові протоколи розподілення ключів з одиночними квантовими системами

Згідно з запропонованою класифікацією відомих на даний час квантових протоколів розподілення ключів (КПРК) з дискретними квантовими станами (рис. 1), можна виділити чотири основні групи таких протоколів:

1) протоколи з використанням одиночних кубітів, які називають також протоколами типу «приготовлення – вимірювання»;

2) протоколи з використанням переплутаних станів кубітів;

3) протоколи з використанням одиночних багаторівневих квантових систем – кудитів;

4) протоколи з використанням переплутаних станів кудитів.

В принципі, протоколи з кубітами можна було б не виділяти в окремі групи. Але такі протоколи, як з одиночними, так і з переплутаними кубітами, історично були розроблені першими. Більшість експериментів на даний час виконано якраз для таких протоколів. Також існуючи на даний час комерційні системи квантового розподілення ключів реалізують поки що тільки протоколи з кубітами. Тому наведена вище класифікація представляється нам найбільш точною.

Розглянемо спочатку групу протоколів, що ґрунтуються на пересиланні одиночних кубітів. У таких протоколах кожний фотон несе один біт інформації.

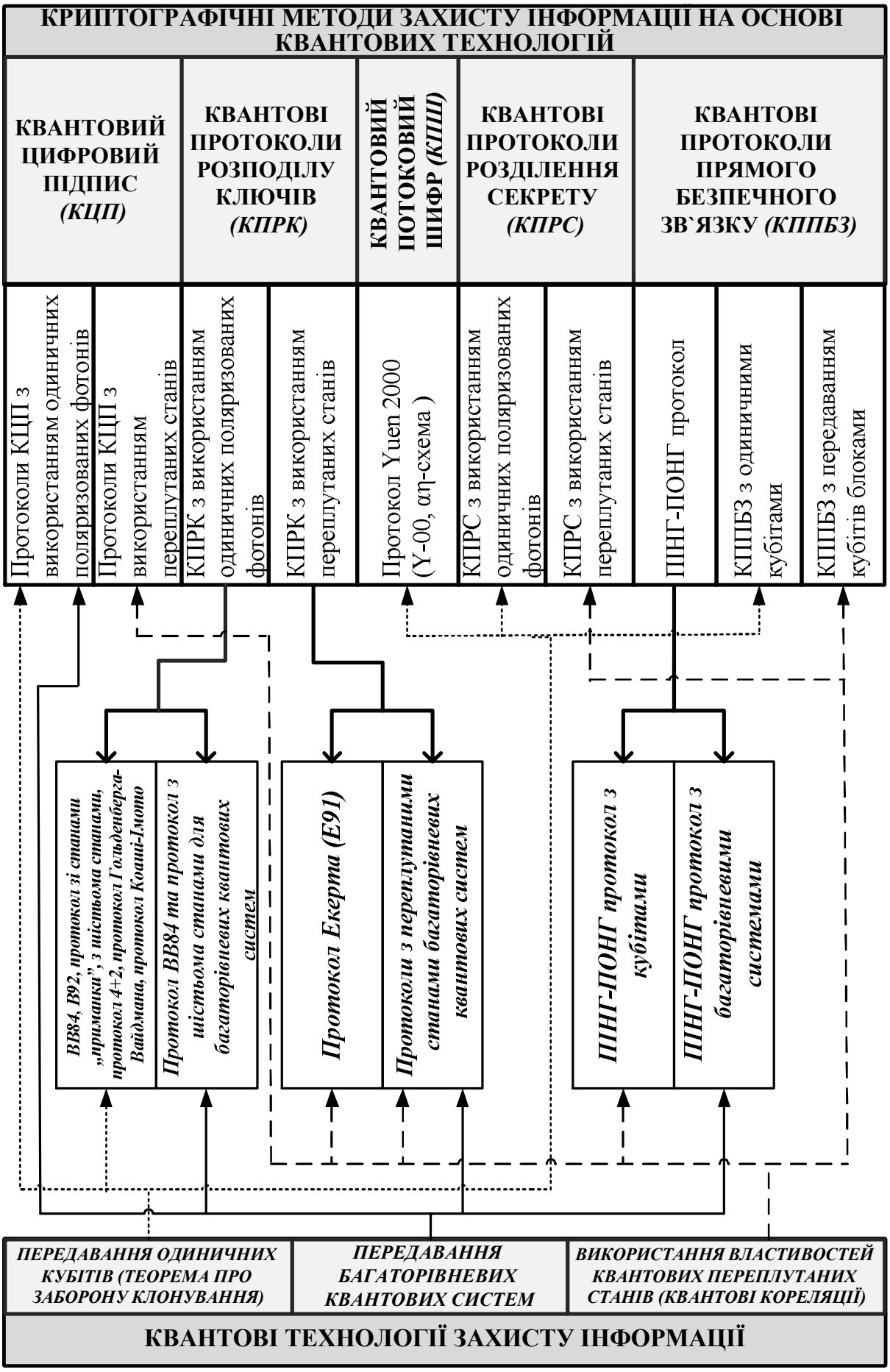


Рис. 1. Класифікація квантових методів захисту інформації

Перший протокол цього типу був запропонований Ч.Х. Бенетом і Ж. Брасаром у 1984 р., згодом він одержав назву BB84 [1]. У цьому протоколі використовують два взаємно незміщених поляризаційних базиси: вертикально–горизонтальний, позначимо його $\oplus$, що відповідає вертикальної (двійковий «0») або горизонтальної (двійкова «1») лінійної поляризації фотонів, і діагональний $\otimes$, що відповідає двом діагональним поляризаціям +45° та –45°. Відзначимо, що взаємно незміщеними (додатковими) називають базиси, для яких будь-які два базисні вектори e_i та e_j, що відносяться до різних базисів, задовольняють співвідношенню $\langle e_i | e_j \rangle = 1/\sqrt{d}$, де d – розмірність гільбертова простору квантової системи ($d = 2$ для кубітів).

Далі будемо використовувати такі позначення суб'єктів протоколу: суб'єкт A – відправник повідомлення, суб'єкт B – отримувач, суб'єкт E – агент, що виконує атаку пасивного перехоплення.

Суб'єкт A випадковим чином вибирає базис і поляризацію своїх однофотонних імпульсів і посилає їх суб'єктові B, тобто суб'єкт A з однаковою ймовірністю посилає один із чотирьох квантових станів:

$$|0\rangle, \quad |1\rangle, \quad |+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right), \quad |-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right). \tag{3}$$

Випадкова поляризація вибирається тому, що ключ повинен бути випадковою послідовністю бітів, а два базиси потрібні для того, щоб перешкодити зловмиснику правильно реєструвати поляризацію фотонів. Приклад стадій протоколу BB84 показаний на рис. 2 [1].

Базис ***A***	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$
Значення біта ***A***	0	1	0	1	1	0	1	0	0	0	0
A посилає	$\|\nearrow\rangle$	$\|\leftrightarrow\rangle$	$\|\updownarrow\rangle$	$\|\searrow\rangle$	$\|\leftrightarrow\rangle$	$\|\nearrow\rangle$	$\|\searrow\rangle$	$\|\updownarrow\rangle$	$\|\nearrow\rangle$	$\|\nearrow\rangle$	$\|\updownarrow\rangle$
Базис ***B***	$\otimes$	$\oplus$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\oplus$
Біт ***B***	0	1	0	0	1	0	1	1	0	1	0
Той же базис?	так	так	ні	ні	так	так	так	ні	ні	ні	так
В ***A*** залишається	0	1			1	0	1				0
В ***B*** залишається	0	1			1	0	1				0
Перевірка ***E***	так	ні			так	ні	ні				ні
Ключ		1				0	1				0

Рис. 2. Приклад стадій протоколу BB84

Для кожного фотона суб'єкт B випадковим чином вибирає базис і вимірює поляризацію в обраному базисі. Отриманий суб'єктом B набір бітів називають сирим ключем. Потім він повідомляє суб'єктові A по відкритому каналу, який базис він використав для кожного вимірювання (зрозуміло, не повідомляючи результати вимірювань). Суб'єкт A повідомляє, який базис використав він. Оскільки суб'єкт B вгадує базис, обраний суб'єктом A, у середньому в половині випадків, то в результаті він правильно приймає близько половини бітів, посланих суб'єктом A. Суб'єкти A і B

відкидають всі біти, що відповідають випадкам, коли вони використовували різні базиси й у результаті одержують просіяний ключ. Інформаційна місткість протоколу BB84 дорівнює відношенню середньої довжини просіяного ключа до середньої довжини сирого і при відсутності завад у квантовому каналі дорівнює 50%.

Далі проводиться процедура виправлення помилок, оцінка їх рівня та оцінка кількості інформації, що могла утекти до зловмисника [1]. Існують різні види атак на протоколи квантового розподілення ключів. Зокрема, на протокол BB84 можливі атаки, що використовують недосконаліть обладнання та не завжди можуть бути виявлені легітимними користувачами [24]. Для виявлення атак, які можливі при використанні суб'єктом A ідеальних однофотонних джерел сигналів, легітимні користувачі повинні оцінити рівень помилок, пожертвував при цьому частиною переданих бітів (ця процедура показана на рис. 2). Після виправлення помилок суб'єкт A й суб'єкт B з високою ймовірністю мають ідентичний погоджений ключ.

Останній етап стеку квантових протоколів розподілення ключів – процедура підсилення секретності, яка забезпечує теоретико-інформаційну стійкість [1, 2]. Суб'єкти A і B визначають величину τ – число бітів, на яке потрібно скоротити погоджений ключ, щоб зробити інформацію зловмисника про ключ нижче заданої малої величини. Потім суб'єкт A генерує випадкову двійкову матрицю K розміру $(n-\tau)\times n$ й відкрито передає її суб'єктові B. Кінцевий секретний ключ (довжини $n-\tau$) тоді виходить множенням (за модулем 2) матриці K на узгоджений ключ довжини n (процедура хешування). При цьому можна строго довести, що при даному τ інформація зловмисника про ключ буде нижче деякого певного значення. Останнє можна вибрати як завгодно малим (природно, що чим менше інформації повинне залишитись у зловмисника, тим більше буде τ й, відповідно, тим коротше буде кінцевий секретний ключ).

В протоколі BB84 для виявлення атаки використовують два взаємно незміщених базиси. Але кількість таких базисів для d-вимірної квантової системи дорівнює $d+1$. Відповідно, для кубітів існує три взаємно незміщених базиси. Протокол, схема якого аналогічна BB84, але в якому використовуються три взаємно незміщених базиси, тобто до чотирьох станів (6) додають ще два, відповідні правої та лівої колової поляризації фотонів, називається протоколом з шістьома станами [2]. Було показано, що стійкість цього протоколу до деяких атак дещо вища за стійкість BB84 [25], але його інформаційна місткість менше та дорівнює 33%.

В 1992 р. Ч.Х. Бенетом був запропонований протокол з одиночними фотонами, де замість поляризації використовується фазове кодування. Цей протокол отримав назву B92. Така система менш піддана завадам, що виникають в оптичному хвилеводі при передачі фотонів, але зловмисник може одержати більше інформації про ключ для заданого рівня створюваних ним помилок, ніж у протоколі BB84, тобто стійкість протоколу B92 нижче за стійкість протоколу BB84. Інформаційна місткість протоколу B92 також нижче за інформаційну місткість BB84 і становить 25% в ідеальному квантовому каналі.

Протокол $4+2$ є гібридним варіантом протоколів BB84 та B92. У ньому використовуються чотири квантових стани для кодування «0» та «1» у двох базисах. Стани в кожному базисі вибираються неортогональними, крім того, стани в різних базисах також мають бути попарно неортогональними. Цей протокол має більш високий рівень стійкості, ніж протокол BB84, коли використовують слабкі когерентні імпульси замість одиночних фотонів, що зараз і відбувається на практиці. Але інформаційна місткість протоколу 4+2 нижче, ніж інформаційна місткість протоколу BB84.

Протоколи зі станами «приманки» (*decoy states protocols*) [21, 26] є удосконаленим варіантом протоколу BB84. У таких протоколах, крім інформаційних сигналів, джерело суб'єкта A також випромінює додаткові імпульси (приманки), у яких середнє число фотонів відрізняється від середнього числа фотонів в інформаційних сигналах.

Атака зловмисника змінює статистичні характеристики станів приманки та/або інформаційних станів і таким чином може бути виявлена. Як показали практичні експерименти, для цих протоколів швидкість передавання ключа й практична довжина каналу більше, ніж для протоколу BB84 [21].

Одним зі шляхів збільшення інформаційної місткості квантових протоколів розподілення ключів є використання для передачі замість дворівневих квантових систем (кубітів) багаторівневих систем (кудитів). Кожний кудит дозволяє передати $\log_2 d$ біт класичної інформації, де d – розмірність гільбертова простору кудита. На даний час запропоновані два види протоколів з одиночними кудитами: перший є узагальненням протоколу BB84, в ньому для забезпечення секретності використовуються два базиси [27]; другий є узагальненням протоколу з шістьома станами, в ньому використовуються $d+1$ базиси [28]. Ефективність протоколів першого типу дорівнює $\log_2 d/2$ біт/кудит, другого типу – $\log_2 d/(d+1)$ біт/кудит.

Квантовий протокол розподілення ключів з переплутаними кубітами

Цей протокол був запропонований А. Екертом у 1991 році [29]. Розподілення ключа виконується через квантовий канал, який містить джерело, що випускає переплутану пару фотонів у синглетному стані (3). Фотони розлітаються в різні сторони (уздовж деякої осі *z*) у напрямку до двох легітимних користувачів каналу, суб'єкта *A* та суб'єкта *B*, які після одержання фотонів виконують вимірювання й реєструють результат цих вимірювань в одному з трьох базисів, одержуваних обертанням $\oplus$-базису навколо осі *z* на деякі заздалегідь визначені кути. При цьому значення кутів повороту базисів повинні бути однаковими в суб'єктів *A* і *B* у двох випадках із трьох, наприклад, в суб'єкта А: $\varphi_1^A = 0$, $\varphi_2^A = \pi/4$, $\varphi_3^A = \pi/8$; в суб'єкта *B*: $\varphi_1^B = 0$, $\varphi_2^B = -\pi/8$, $\varphi_3^B = \pi/8$. Конкретний базис для кожного вимірювання обидва вони вибирають випадково й незалежно один від одного.

Після того, як відбулася передача, суб'єкти *A* і *B* можуть публічно оголосити, які орієнтації базисів вони вибирали в кожному конкретному випадку, і розділити проведені вимірювання на дві різні групи: у першій групі будуть вимірювання, у яких вони використали різні орієнтації базисів, а в другий – ті, у яких орієнтації базисів збігалися. Вони також відкидають всі випадки, коли один з них або обидва взагалі не змогли зареєструвати жодного фотона. Таким чином, при відсутності завад в каналі інформаційна місткість протоколу Екерта дорівнює 2/9 біт на пару кубітів, оскільки випадки використання різних базисів використовуються тільки для контролю підслуховування й відкидаються при просіюванні ключа.

Після цього суб'єкти *A* і *B* можуть відкрито показати один одному результати, які вони одержали в рамках однієї тільки першої групи вимірювань, тобто коли орієнтації їхніх базисів не збігалися. Це дозволяє їм установити коефіцієнт кореляції вимірювань *S*, який також може бути обчислений з використанням законів квантової механіки [1]:

$$S = E\left(\varphi_1^A, \varphi_2^B\right) + E\left(\varphi_1^A, \varphi_3^B\right) + E\left(\varphi_2^A, \varphi_3^B\right) - E\left(\varphi_2^A, \varphi_2^B\right), \qquad (4)$$

де $E\left(\varphi_i^A, \varphi_j^B\right) = -\cos\left(2\left(\varphi_i^A - \varphi_j^B\right)\right)$.

При використанні наведених вище значень кутів повороту базисів у суб'єктів *A* і *B*, з (4) одержуємо $S = -2\sqrt{2}$. Якщо значення *S*, отримане в результаті вимірювань суб'єктів *A* і *B* при використанні ними різних базисів, дорівнює $-2\sqrt{2}$, то стани фотонів із переплутаних пар не були змінені на шляху від джерела до легітимних користувачів. Отже, результати, отримані в другій групі вимірювань, тобто коли

суб'єкти *A* і *B* використали однакові базиси, антикорелюють і можуть бути перетворені в секретний рядок бітів – ключ.

Якщо ж отримана величина *S* не дорівнює $-2\sqrt{2}$, то це означає, що стани фотонів були змінені, або в результаті перехоплення, або в результаті завад у квантовому каналі зв'язку. Далі суб'єкти *A* і *B* повинні оцінити рівень помилок і або визнати його прийнятним і провести процедуру квантового підсилення секретності [1], що дозволить їм встановити секретний ключ, або, якщо рівень помилок неприйнятний, то незалежно від їхньої природи – наявності атаки зловмисника, або наявності завад у каналі – потрібно повторити всю процедуру знову.

На сьогодні запропоновані узагальнення протоколу Екерта на випадок використання переплутаних пар кудитів [30, 31]. Ці протоколи мають більшу стійкість до деяких атак та більшу інформаційну місткість порівняно з оригінальним протоколом Екерта.

Відзначимо, що однією з головних концептуальних переваг протоколів з переплутаними станами квантових систем над протоколами з одиночними квантовими системами є випадковість результатів квантових вимірювань над переплутаними системами, в результаті чого легітимні користувачі отримують повністю випадковий спільний ключ. При використанні протоколів з одиночними квантовими системами суб'єкт *A* повинен спочатку згенерувати випадковий ключ. Відзначимо, що на даний час існують комерційні квантові генератори випадкових чисел, наприклад, генератор *QUANTIS* швейцарської компанії Id Quantique [32], який може використовуватись для генерації істино випадкового криптографічного ключа.

Комерційні квантові системи розподілення ключів, переваги та недоліки квантового розподілення ключів

Першою комерційною системою квантового розподілення ключів була *QPN Security Gateway* (*QPN-8505*) [33], створена компанією MagiQ Technologies (США). Дана система представляє собою економічно ефективне рішення інформаційної безпеки для державних і фінансових організацій. Система пропонує захист віртуальних приватних мереж за допомогою квантового розподілення ключів (до ста 256 бітних ключів у секунду на відстань до 140 км) та інтегрованого шифрування. Для квантового розподілення ключів *QPN-8505* використовує протокол BB84 з фазовим кодуванням, а для шифрування даних – симетричний шифр AES.

Швейцарська компанія Id Quantique пропонує системи *Clavis*^{2} і *Cerberis* [34]. *Clavis*^{2} використовує власну автокомпенсувальну оптичну платформу, яка має високу стабільність, що гарантує низький рівень квантових помилок. Безпечний обмін ключами можливий на відстані до 100 км. Ця оптична платформа добре документована в наукових публікаціях і була ретельно протестована. *Cerberis* являє собою сервер з автоматичним створенням і секретним обміном ключами через оптоволоконний канал. Дана система може передавати криптографічні ключі на відстань до 50 км, її характерною особливістю є 12 паралельних криптографічних обчислень, що значно підвищує швидкодію. Система *Cerberis* використовує шифр AES з ключем довжиною 256 біт, а для квантового розподілення ключів – протоколи BB84 та SARG.

Нещодавно компанією Toshiba Research Europe Ltd (Великобританія) було представлено ще одну систему квантового розподілення ключів під назвою *Quantum Key Server* [35]. Ця система забезпечує генерацію до ста 256 бітних ключів за секунду та їх передавання на відстань понад 100 км. При передаванні на відстань до 50 км забезпечується швидкість 1 Мбіт/с. До складу *Quantum Key Server* входить інтегрований модуль автоматичного управління, який проводить неперервний моніторинг системи та регулює її оптичні характеристики.

Ще одна британська компанія QinetiQ представила першу у світі мережу, що використовує квантову криптографію – *Quantum Net* (*Qnet*) [36]. Максимальна довжина ліній зв'язку даної мережі становить 120 км, та найголовнішим є те, що система *Qnet* – це перша квантово-криптографічна система, що використовує більше двох серверів. Їх в даній системі шість і всі вони є інтегрованими в мережу Internet.

Підсумовуючи аналіз виконаних на даній час теоретичних та експериментальних досліджень в галузі квантового розподілення ключів, можна виділити наступні їх переваги та недоліки.

Переваги:

1) Протоколи квантового розподілення ключів дозволяють виявити атаку пасивного перехоплення, так як підключення зловмисника, як правило, вносить до квантового каналу значно більший рівень помилок порівняно з рівнем природніх завад у каналі (за виключенням деяких специфічних атак, які використовують недосконаліть конкретного обладнання, наприклад, дуже високий рівень завад у каналі, або недосконаліть деяких типів датчиків фотонів [37]).

2) Процедура підсилення секретності, що виконується у протоколах квантового розподілення ключів, дозволяє при визначеній умові досягти безумовної (теоретико-інформаційної) стійкості розподілення ключів, яка не досягається при використанні для розподілення ключів методів асиметричної криптографії, наприклад, схеми Діффі-Геллмана. Умова досягнення безумовної стійкості полягає у тому, що після завершення квантового передавання взаємна інформація між легітимними користувачами повинна бути більшою за взаємну інформацію між легітимним користувачем та зловмисником.

3) Безумовна (теоретико-інформаційна) стійкість квантових протоколів розподілення ключів дозволяє використати абсолютно секретний ключ для подальшого шифрування відомими класичними симетричними шифрами – це відповідно збільшує рівень захищеності, який забезпечують суто класичні криптосистеми. Також можливий синтез квантових протоколів розподілення ключів з шифром Вернама (одноразовим блокнотом), що в поєднанні з безумовно стійкою схемою автентифікації дозволить створити абсолютно стійку систему передавання конфіденційної інформації.

Недоліки:

1) Система, що побудована тільки на квантових протоколах розподілення ключів, не може слугувати повноцінним завершеним рішенням проблеми розподілення секретних ключів – потрібні також засоби для попередньої автентифікації користувачів. Така автентифікація може бути виконана, наприклад, за допомогою начального невеликого секретного ключа, який користувачі системи квантового розподілення ключів повинні отримати один раз заздалегідь. Потім невелику частку секретного ключа, розподіленого за допомогою квантового протоколу, користувачі можуть залишити для автентифікації в наступному сеансі тощо.

2) Обмеження довжини квантового каналу: при квантовому передаванні інформації неможливо «підсилити сигнал» через неможливість копіювання квантових станів. Проте, можна створити квантовий аналог повторювача, що дає можливість квантового передавання інформації на великі відстані за допомогою створення переплутаних станів між відправником та одержувачем. Це переплутування потім може бути використано при квантовій комунікації, зокрема в квантових протоколах розподілення ключів. Технологія квантових повторювачів, яка ґрунтується на використанні квантової пам'яті, активно розробляється на даний час, але ця технологія поки ще не вийшла за межі лабораторних експериментів.

3) Низька ефективність (ймовірність зареєструвати відлік, якщо фотон попав у детектор) детекторів одиночних фотонів – для телекомунікаційного «вікна прозорості» 1550 нм ефективність таких детекторів, що працюють при температурах 200-300 К, не перевищує 10% [37]. Існують також надпровідні детектори, що працюють при над низьких температурах 0.1-1.5 К, ефективність яких досягає 95% [37]. Але використання

таких надпровідних детекторів у квантових системах розподілення ключів значно збільшує вартість системи. Ще одна проблема, яка пов'язана з детекторами, – ефект «темнового шуму», коли детектор спрацьовує при відсутності фотону [37].

4) Швидкість передавання інформації квантовим каналом суттєво зменшується зі збільшенням довжини каналу й в більшості експериментів на відстанях порядку 100-150 км дорівнює декільком кілобітам за секунду.

5) Деполяризація фотонів у квантовому каналі, яка призводить до помилок при вимірюваннях у легітимних користувачів.

6) Висока ринкова ціна існуючих на сьогодні комерційних систем квантового розподілення ключів.

Висновки

На сьогодні квантове розподілення ключів є найбільш розвиненою галуззю квантової криптографії. Технологія квантового розподілення ключів дозволяє розподіляти секретні ключі з дуже високим ступенем безпеки. У науково-дослідних інститутах та лабораторіях розвинених країн вже розроблені готові системи для квантового розподілення ключів. Такі системи можуть бути об'єднані з будь-якою класичною системою шифрування, яка забезпечує теоретико-інформаційну стійкість, і при цьому така комплексна система шифрування також буде мати теоретико-інформаційну стійкість. Взагалі, протоколи квантового розподілення ключів можуть забезпечити вищий рівень безпеки, ніж відповідні класичні схеми.

У той же час системи квантового розподілення ключів, хоча і можуть вже зараз бути інтегрованими в існуючу інфраструктуру мереж передачі даних, але мають й низку недоліків. Більшість цих недоліків мають технологічний характер і можуть бути усунені в майбутньому. Однак на даний час технологія квантового розподілення ключів є ще досить «сирою» і дорогою, що обмежує її застосування галузями, де вартість не є головним чинником, але потрібний високий рівень безпеки, наприклад, у системах урядового та військового зв'язку. Варто також відзначити, що наявні на цей час комерційні квантові системи розподілення ключів містять досить складні оптоволоконні, електронні та програмні компоненти, робота з якими є, скоріше, проведенням складного наукового експерименту, ніж практичною діяльністю із використанням загальновживаного й стандартного встаткування. Цей факт також є поки серйозним обмеженням для широкого поширення систем квантового розподілення ключів.

Інші напрями квантової криптографії на теперішній час ще не вийшли за межі лабораторних експериментів. Але вже запропоновано велику кількість теоретичних схем, для яких доведено їх високу стійкість, аж до теоретико-інформаційної. Так, наприклад, квантові протоколи прямого безпечного зв'язку взагалі знімають проблему розподілення секретних ключів, так як зовсім не використовують шифрування. Але один з класів таких протоколів – пінг-понг протокол та його вдосконалені варіанти, – забезпечує тільки асимптотичну безпеку (без використання додаткових методів підсилення його безпеки), а інший клас – протоколи з передаванням кубітів блоками – потребує наявності квантової пам'яті, яка поки що знаходиться за межами сучасних технологій [6].

Таким чином, квантові технології захисту інформації бурхливо розвиваються в останні роки та поступово займають своє місце серед інших засобів, що обумовлено їх високим рівнем стійкості та властивостями, яких немає у класичних засобів захисту інформації. Але для практичного використання квантових технологій захисту інформації в ІКТ необхідно вирішити ще ряд завдань як теоретичного, так і, в першу чергу, практичного характеру.

Список літератури

1. Физика квантовой информации [Текст] : Квантовая криптография. Квантовая телепортация. Квантовые вычисления / пер. с англ. С.П. Кулик, Е.А. Шапиро ; ред. пер. С.П. Кулик, Т.А. Шмаонов ; ред. Д. Боумейстер [и др.]. – М. : Постмаркет, 2002. – С. 33-73.
2. Gisin N. Quantum cryptography / N. Gisin, G. Ribordy, W. Tittel, H. Zbinden // Review of Modern Physics. – 2002. – Vol.74, Iss.1. – PP. 145-195.
3. Applied Quantum Cryptography / C. Kollmitzer, M. Pivk (eds.). // Lecture Notes in Physics 797. – Springer-Verlag, Berlin, Heidelberg, 2010. – 242 p.
4. Korchenko O. Quantum Secure Telecommunication Systems / O. Korchenko, P. Vorobiyenko, M. Lutskiy, Ye. Vasiliu, S. Gnatyuk // Telecommunications Networks – Current Status and Future Trends (Edited by J.H. Ortiz). – InTech, 2010. – PP. 211-236.
5. Василиу Е.В. Проблемы развития и перспективы использования квантово-криптографических систем / Е.В. Василиу, П.П. Воробиенко // Наукові праці ОНАЗ ім. О.С. Попова. – 2006. – №1. – С. 3-17.
6. Корченко О.Г. Сучасні квантові технології захисту інформації / О.Г. Корченко, Є.В. Василіу, С.О. Гнатюк // Науково-технічний журнал «Захист інформації». – 2010. – №1. – С. 77-89.
7. Boström K. Deterministic Secure Direct Communication Using Entanglement / K. Boström, T. Felbinger // Physical Review Letters. – 2002. – Vol.89, Iss.18. – 187902.
8. Ostermeyer M. On the implementation of a deterministic secure coding protocol using polarization entangled photons / M. Ostermeyer, N. Walenta // Optics Communications. – 2008. – Vol.281, Iss.17. – PP. 4540-4544.
9. Vasiliu E.V. Non-coherent attack on the ping-pong protocol with completely entangled pairs of qutrits / E.V. Vasiliu // Quantum Information Processing. – 2011. – Vol.10, No.2. – PP. 189-202.
10. Василіу Є.В. Синтез структури квантових систем прямого безпечного зв'язку / Є.В. Василіу // Цифрові технології. – 2011. – №9. – С. 20-30.
11. Hillery M. Quantum secret sharing / M. Hillery, V. Bužek, A. Berthiaume // Physical Review A. – 1999. – Vol.59, Iss.3. – PP. 1829-1834.
12. Yan F.-L. Quantum Secret Sharing Protocol between Multiparty and Multiparty with Single Photons and Unitary Transformations / F.-L. Yan, T. Gao, Yu.-Ch. Li // Chinese Physics Letters. – 2008. – Vol.25, No.4. – PP. 1187-1190.
13. Hirota O. Quantum stream cipher by the Yuen 2000 protocol: Design and experiment by an intensity-modulation scheme / O. Hirota, M. Sohma, M. Fuse, and K. Kato // Physical Review A. – 2005 – Vol.72, Iss.2. – 022335.
14. Corndorf E. Quantum-noise randomized data encryption for wavelength-division-multiplexed fiber-optic networks / E. Corndorf, C. Liang, G.S. Kanter, *et al.* // Physical Review A. – 2005. – Vol.71, Iss.6. – 062326.
15. Wang J. Quantum signature scheme with single photons / J. Wang, Q. Zhang, and C.J. Tang // Optoelectronics Letters. – 2006. – Vol.2, No.3. – PP. 209-212.
16. Gottesman D. Quantum digital signatures: [Електронний ресурс] / D. Gottesman, I. Chuang. – Режим доступу: http://arxiv.org/abs/quant-ph/0105032 (Дата звернення: 26.07.2012).
17. Natori S. Why Quantum Steganography Can Be Stronger Than Classical Steganography / S. Natori // Quantum Computation and Information. Topics in Applied Physics. – 2006. – Vol.102. – PP. 235-240.
18. Martin K. Steganographic communication with quantum information / K. Martin // Information Hiding, Lecture Notes in Computer Science. – 2007. – Vol.4567. – PP. 32-49.
19. Конахович Г.Ф. Сучасні методи квантової стеганографії / Г.Ф. Конахович, О.В. Шевченко, В.М. Кінзерявий, Ю.Є. Хохлачова // Науково-технічний журнал «Захист інформації». – 2011. – Том 2, №51. – С. 82-86.
20. Lo H.-K. Quantum cryptography / H.-K. Lo, Y. Zhao // Encyclopedia of Complexity and Systems Science. – New York: Springer US, 2009. – Vol.8. – PP. 7265-7289.
21. Peng C.-Z. Experimental Long-Distance Decoy-State Quantum Key Distribution Based on Polarization Encoding / C.-Z. Peng, J. Zhang, D. Yang, *et al.* // Physical Review Letters. – 2007. – Vol.98, Iss.1. – 010505.
22. Zhang Q. Megabits secure key rate quantum key distribution / Q. Zhang, H. Takesue, T. Honjo, *et al.* // New Journal of Physics. – 2009. – Vol.11, Iss.4. – 045010.
23. Yuan Z.L. Practical gigahertz quantum key distribution based on avalanche photodiodes / Z.L. Yuan, A.R. Dixon, J.F. Dynes, *et al.* // New Journal of Physics. – 2009. – Vol.11, Iss.4. – 045019.
24. Корченко О.Г. Атаки в квантових системах захисту інформації / О.Г. Корченко, Є.В. Василіу, С.О. Гнатюк, В.М. Кінзерявий // Вісник інженерної академії України. – 2010. – №3-4. – С. 124-133.

25. Bruss D. Optimal Eavesdropping in Quantum Cryptography with Six States / D. Bruss // Physical Review Letters. – 1998. – Vol.81, Iss.14. – PP. 3018-3021.
26. Scarani V. The security of practical quantum key distribution / V. Scarani, H. Bechmann-Pasquinucci, N.J. Cerf, *et al.* // Review of Modern Physics. – 2009. – V.81, Iss.3. – PP. 1301-1350.
27. Cerf N.J. Security of Quantum Key Distribution Using *d*-Level Systems / N.J. Cerf, M. Bourennane, A. Karlsson, N. Gisin // Physical Review Letters. – 2002. – Vol.88, Iss.12. – 127902.
28. Bourennane M. Quantum Key Distribution Using Multilevel Encoding / M. Bourennane, A. Karlsson, G. Björk // Quantum Communication, Computing, and Measurement 3. – New York: Springer US, 2002. – PP. 295-298.
29. Ekert A. Quantum cryptography based on Bell's theorem / A. Ekert // Physical Review Letters. – 1991. – Vol.67, Iss.6. – PP. 661-663.
30. Durt T. Security of quantum key distributions with entangled qudits / T. Durt, D. Kaszlikowski, J.-L. Chen, L.C. Kwek // Physical Review A. – 2004. – Vol.69, Iss.3. – 032313.
31. Василиу Е.В. Анализ стойкости к некогерентной атаке четырех квантовых протоколов распределения ключей с кутритами / Е.В. Василиу // Науково-технічний журнал «Захист інформації». – 2010. – Том 2, №47. – С. 20-26.
32. QUANTIS: True Random Number Generator Exploiting Quantum Physics: *[Електронний ресурс]* // ID Quantique SA. Genève, Switzerland. Режим доступу: http://www.idquantique.com/true-random-number-generator/products-overview.html (Дата звернення: 26.07.2012).
33. QPN Security Gateway (QPN–8505): *[Електронний ресурс]* // MagiQ Technologies. Boston, USA, 2002-2012. Режим доступу: http://www.magiqtech.com/MagiQ/Products.html (Дата звернення: 26.07.2012).
34. Cerberis. A Fast And Secure Solution: High Speed Encryption Combined With Quantum Key Distribution: *[Електронний ресурс]* // ID Quantique SA. Genève, Switzerland. Режим доступу: http://www.idquantique.com/products/cerberis.htm (Дата звернення: 26.07.2012).
35. QKS. Toshiba Quantum Key Distribution System: *[Електронний ресурс]* // Toshiba Research Europe Ltd., Cambridge Research Laboratory. Режим доступу: http://www.toshiba-europe.com/research/crl/qig/quantumkeyserver.html (Дата звернення: 26.07.2012).
36. Elliott C. Quantum Cryptography in Practice / C. Elliott, D. Pearson, G. Troxel // SIGCOMM' 03: Proceedings of the 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications. – New York: ACM Press, 2003. – PP. 227-238.
37. Hadfield R.H. Single-photon detectors for optical quantum information applications / R.H. Hadfield // Nature Photonics. – 2009. – Vol.3, No.12. – PP. 696-705.

СОВРЕМЕННЫЕ КВАНТОВЫЕ ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СИСТЕМАХ

Е.В. Василиу

Одесская национальная академия связи им. А.С. Попова,
ул. Кузнечная, 1, Одесса, 65029, Украина; e-mail: vasiliu@te.net.ua

В статье на основе выполненных ранее систематизации и классификации квантовых технологий защиты информации представлена характеристика основных направлений современной квантовой криптографии с точки зрения используемых квантовых технологий. Рассмотрены основные свойства квантовых систем, которые используются в квантовой криптографии. Приведено краткое описание основных типов квантовых протоколов распределения ключей, выполнен детальный анализ их преимуществ и недостатков. Рассмотрено текущее состояние проблемы практического использования квантовой криптографии в информационно-коммуникационных системах, в частности, дан краткий обзор существующих коммерческих систем квантового распределение ключей.

Ключевые слова: квантовая криптография, кубит, кудит, свойства квантовых систем, квантовые протоколы распределения ключей, коммерческие системы квантовой криптографии

MODERN QUANTUM TECHNOLOGIES OF THE INFORMATION PROTECTION IN INFORMATION-COMMUNICATION SYSTEMS

Eugene V. Vasiliu

Odessa National Academy of Telecommunication n.a. O.S. Popov,
1 Koval'ska str., Odesa, 65029, Ukraine; e-mail: vasiliu@te.net.ua

In the paper on the basis of systematization and classification of quantum technologies of the information protection, carried out before, the characteristic of the basic directions of modern quantum cryptography from the point of view of used quantum technologies is presented. The basic properties of quantum systems which are used in quantum cryptography are considered. The short description of the basic types of quantum key distribution protocols is given; the detailed analysis of their advantages and lacks is made. The current status of a problem of practical quantum cryptography using in information-communication systems is considered. In particular, the short review of existing commercial systems of quantum key distribution is given.

Keywords: quantum cryptography, qubit, qudit, properties of quantum systems, quantum key distribution protocols, commercial systems of quantum cryptography

Mathematics Subject Classification (2010) 68M10

Informatics and Mathematical Methods in Simulation
Vol. 2 (2012), No. 2, pp. 113-120

RANDOM CONTROL OF SENDING RADIO MESSAGES IN THE WIRELESS SENSOR NETWORK

Stanisław W. Rajba

University of Bielsko-Biala,
ul. Willowa, 2, 43-309 Bielsko-Biala, Poland; e-mail: rajbas@ath.bielsko.pl

This work presents a method for random control transmission in Wireless Sensor Network (WSN). Specified conditions as the probability of collision-free WSN network transmission of single-hop. Innovativeness of this work lies in the concept of WSN with random times of one-way transmission using one single radio frequency. Network access control is implemented using the Poisson Arrivals See Time Averages (PASTA) for modeling WSN. We determine as well the probability of collisions in the interval of given small length as the probability of given number of times communications by nodes that are in a collision during communication.

Keywords: Wireless Sensor Network (WSN), Poisson Arrivals See Time Averages (PASTA system), probability of collision, random control

Problem formulation

The paper presents the problem of control radio transmission messages generated by nodes in wireless networks, the measurement of random access. The issue of random access control for wireless measurement is examined in terms of small times smaller than the duration of the communication protocol. We study the conditions of communication nodes depending on their number, average transmission time working on the basis of earlier proposed algorithm using a Poisson stream. In particular, we determine as well the probability of collisions in the interval of given small length as the probability of a given number of times communications by nodes that are in a collision during communication, based on the number of nodes and other network communication parameters. It also provides the expected number of nodes that are in collision and the variance.

Evaluation of recent publications in the explored issue

A primary issue in the networks – Wireless Sensor Network (WSN) is to control the emission of many radio broadcasters to one base station so that there was no a collision, or that the probability of collision is sufficiently very small, which is determined by the quality parameters on the teletransmission for a particular application type. Process control emissions of all nodes in addition taking into account the transmission properties of space as the transmission medium for radio waves, can be partly seen on the model of the known methods used in computer networks [4]. Many of these methods is perfectly resolved, but they all have some major drawbacks. These include: the need for two-way transmission between the node and the base station (outlet data). All based on management control process emissions by the base station always requires communication from the base station to a node, and therefore requires facilities of nodes in the receiver control signals in addition to their own transmitters to issue raised by the node information. This situation leads to further difficulties and limitations, as the demand for the number of radio channels as well as the necessary power

supply nodes. You can create and use channels of division frequency (seems the most natural), but also time-division and code division). All these techniques are well known in the telecommunications and professional systems used in telecommunications, but in the case of WSN network new ones entirely different problems, which in traditional telecommunication systems do not occur. These include: reduced power and capacity of the power source nodes. Nodes are usually mobile and do not have the traditional power supply. Too small number of channels you can create in a limited space with significant numbers of nodes, typically much higher demand for radio channels than in conventional systems - such as mobile phones [11].

In this context, an interesting proposal is to implement the network that broadcast radio messages of the nodes is carried out to the base station using only one frequency, and one-way. Simplex transmission from the node to the base station does not allow the process to control emissions from the base station therefore sought a mechanism for controlling the radio emission of each node should provide a collision-free broadcast nodes that do not correspond with each other and not any contact between them is to organize the process of transmission. Traditional methods can not solve the problem with such restrictions, which in turn are a very serious advantages WSN network.

In this paper we offer a random way to control the transmission process – using Poisson Arrivals See Time Averages (PASTA) [12, 13]. In the proposed method of execution control, we agree to a number of possible collisions of radio, but the probability of correct transmission and control parameters are selected randomly by the emission process of pre-established requirements.

Network model

We analyze a network consisting of n sensors which are able to send information about the measured physical magnitude on one selected radio frequency to the receiving base, quite independently of each other. Duration of communication protocol is t_p, the sensors send the information to the receiving point in randomly selected moments, every T s. at a average.

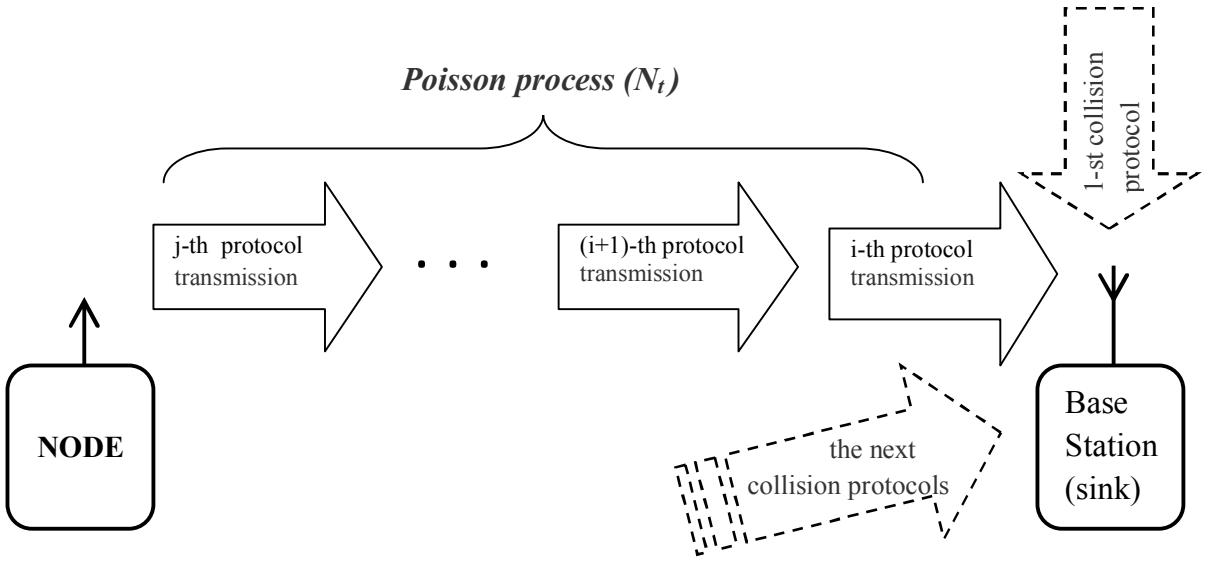


Fig. 1. Poisson modeling of network transmission protocols in WSN

Beginning and cessation of transmission of a particular sensor takes place in random moments of time but these moments are relatively rare. It is a one-way transmission, i.e. from sensors to the receiving base. The sensors are completely independent of one another and their

on or off state is of no influence on the operation of the network. All the sensor- senders or a part of them may be mobile provided that their senders have been left within the radio range of the receiving base. If one or more senders start sending while protocol transmission of t_p time is going on from another sensor, then such a situation is called collision. Collision excludes the possibility of the correct receiving of information by the receiving base. Such a disturbed signal is ignored. The receiving base rejects the erroneous message and waits for a retransmission to be made after the average time T. We must accept a certain loss of information in exchange for simplicity in respect of both system and equipment.

As mentioned in the Introduction, we used to modeling our wireless network a Poisson process. Mathematically the process N is described by so called counter process N_t or $N(t)$ (see [14], and [15, 16]) of rate $\lambda > 0$. The counter tells the number of events that have occurred in the interval $[0,t]$, $(t \geq 0)$. N has independent increments (the number of occurrences counted in disjoint intervals are independent from each other), such that $N(t) - N(s)$ has the Poisson ($\lambda(t-s)$) distribution (mean $\lambda(t-s)$), for $t \geq s \geq 0$, $j = 0,1,2,\ldots$

$$P\{N(t) - N(s) = j\} = e^{-\lambda(t-s)} \frac{[\lambda(t-s)]^j}{j!}. \qquad (1)$$

Let us state our main assumptions. There are n identical sensors observing a dynamical system and reporting to a central location over the wireless sensor network with one radio channel. For simplicity, we assume our sensor network to be a single hop network with star topology. We also assume every node (sender-sensor, shortly sensor) always has packet ready for transmission. We assume that sensors send probe packets at Poissonian times. The average time between sending (the wake-up-times) of a sensor is T (the epoch period), and the duration of the on-time t_p (the awake interval). Assume that the wake-up-times corresponding to sensors are independent each of other. Let N be the Poisson process representing the time counter of sending sensors. We say that a collision occurs in the time interval of t_p length, if at least two sensors start sending within this interval. We say that a collision occurs in time interval s, if there exist at least two sensors which start sending within this interval with the difference between the beginning of their sending time not exceeding the value of t_p.

Then the Poisson process N has the rate $\lambda = n/T$. By (1)

$$P(N_t = j) = e^{-\lambda t} \frac{[\lambda t]^j}{j!}, \; j = 0,1,\ldots \qquad (2)$$

In [16, 17] we give the theorems on the probability of collisions in the interval of s length in the case $s > t_p$. In the next theorem we consider the case $0 < s \leq t_p$. Let A_s, A_s' be the events that denote the collisions occur and the lack of collisions, respectively, in the interval of s length ($s > 0$). Let Y_s be the number sensor transmissions in collision in the interval of s length.

Consider $0 < s \leq t_p$. Let $p(j;s)$, $j = 0,1,2,\ldots$, be the probability that the number of sensor transmissions that have occurred in the interval $[0,s]$ equals j. From (2), we obtain, for $j = 0,1,2,\ldots$

$$p(j;s)=e^{-\lambda s}\frac{[js]^j}{j!}=e^{-n\frac{s}{T}}\frac{\left[n\frac{s}{T}\right]^j}{j!}. \tag{3}$$

In particular cases, for $j=2,3,\ldots$, $p(j;s)$ can be regarded as the probability of exactly j collisions in the interval $[0,s]$, and consequently by the stationarity of Poisson process, in every interval $[t,t+s]$, $(t>0)$.

Now we are going to calculate a probability of collisions in the s-long interval (see Fig. 2, 3).

Theorem 1.

1) The probability of collisions in the interval of s length, where $0<s\le t_p$, is given by the formula:

$$P(A_s)=1-e^{-n\frac{s}{T}}-n\frac{s}{T}e^{-n\frac{s}{T}}.$$

2) The average of the number of sensor transmissions in collision, in the interval of s length, $0<s\le t_p$ is given by the formula:

$$E(Y_s)=\left(1-e^{n\frac{s}{T}}\right)\cdot n\frac{s}{T},$$

where n is the number of sensors, T is the average time between sending of a sensor and t_p is the duration time of a protocol.

Proof: Taking into account that a collision occurs in the time interval of t_p length, if at least two sensors start sending within this interval, by (3) we obtain:

$$P(A_s)=\sum_{j=2}^{\infty}p(j;s)=1-p(0;s)-p(1;s)=1-e^{-n\frac{s}{T}}-n\frac{s}{T}e^{-n\frac{s}{T}}.$$

Note, that the number of sensor transmissions that have occurred in the interval $[0,s]$, i.e. N_s, has a Poisson distribution with the rate $\lambda s=n\frac{s}{T}$. We obtain

$$EN_s=n\frac{s}{T}=\sum_{j=0}^{\infty}jp(j;s)=\sum_{j=1}^{\infty}jp(j;s). \tag{4}$$

Let Y_s be the number sensor transmissions in collision, in the interval $[0,s]$. Then we have

$$P(Y_s=0)=p(0;s)+p(1;s)=e^{-n\frac{s}{T}}+e^{-n\frac{s}{T}}\left[n\frac{s}{T}\right],$$

$$P(Y_s = j) = p(j;s) = e^{-n\frac{s}{T}} \frac{\left[n\frac{s}{T}\right]^j}{j!},\ j = 2,3,\ldots$$

Consequently by (4), we obtain:

$$E(Y_s) = \sum_{k=0}^{\infty} jP(Y_s = j) = \sum_{k=2}^{\infty} jp(j;s) = \sum_{k=1}^{\infty} jp(j;s) - p(1;s) = n\frac{s}{T} - e^{-n\frac{s}{T}} n\frac{s}{T} = \left(1 - e^{-n\frac{s}{T}}\right) \cdot n\frac{s}{T}.$$

This completes the proof of theorem.

Now we are going to get the probability of signal transmission without any collision. Let $P(B_s)$ denote the probability of disturbance of signal transmission (see Fig. 2, 3).

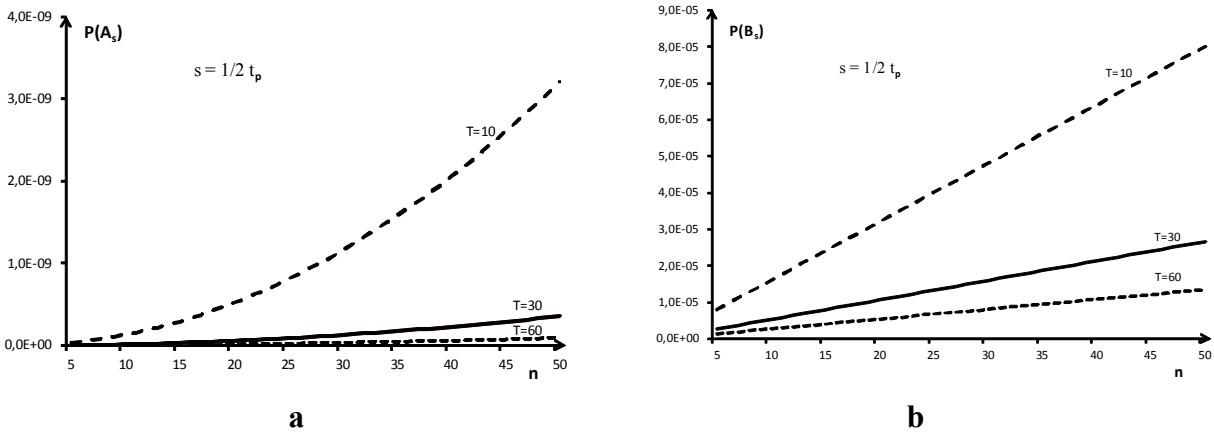
Theorem 2.

The probability of disturbance of signal transmission is given by the formula

$$P(B_s) = 1 - e^{-n\frac{s}{T}}.$$

Proof: Assume that sensor started transmission at some point of time. Note that that this transmission will be without collisions if there is no sensor transmissions within the time interval of t_p length. Then the disturbance of signal transmission occurs in the time interval of t_p length, if at least one sensor start sending within this interval, by (3) we obtain:

$$P(B_s) = \sum_{j=1}^{\infty} p(j;s) = 1 - p(0;s) = 1 - e^{-n\frac{s}{T}}.$$



a **b**

Fig. 2. a) $P(A_s)$ – the collision probability depending on the number of sensors, b) $P(B_s)$ – the probability of disturbance of signal transmission, depending on the number of sensors. Observation time $s = \frac{1}{2}t_p$, $t_p = 3.2 \times 10^{-5}$ s., $T = 10, 30, 60$ s.

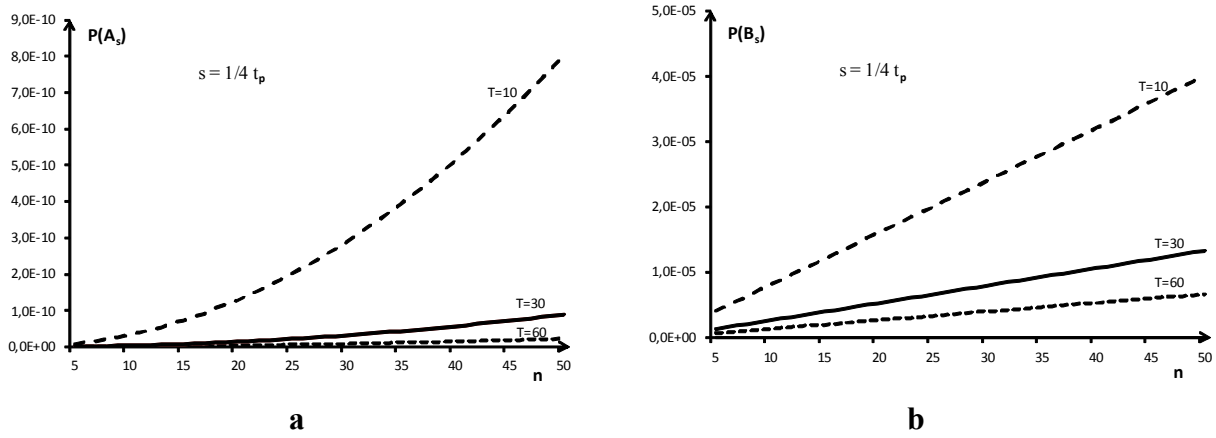


Fig. 3. a) $P(A_s)$ – the collision probability depending on the number of sensors , b) $P(B_s)$ – the probability of disturbance of signal transmission, depending on the number of sensors. Observation time $s = \frac{1}{4}t_p$, $t_p = 3.2 \times 10^{-5}$ s., $T = 10, 30, 60$ s.

Conclusions

The paper analyzes the control random broadcasting WSN nodes. The probability of collisions has been studied in the length of time shorter than the duration of the communication protocol (t_p). In Figures 2 and 3 illustrate the phenomena taking place in practice for different numbers of nodes in the WSN and three times average transmission T (10s., 30s., 60s.), which was adopted to study. The probability $P(A_s)$ illustrates the situation when in the studied time interval $\frac{1}{2}t_p$ (Fig. 2a) and $\frac{1}{4}t_p$ (Fig. 3a), respectively, we examine the probability of collision sent the radio protocols. And so they have a suitable time interval considered, at least two nodes (or more). You can see that the probability of collision is very small (at 10^{-9}-10^{-10}) and depends on the number of nodes in the network and it is not linear. A significant increase in the number of nodes in the network resulting in a significant deterioration in quality. In the case at the situation and was still comfortable for the proper operation of the network. It should, however, reckon with the fact that reducing the average transmission time, increasing the number of nodes in the network get to certain values that prevent the effective use of this method of control. Next, studying the probability $P(B_s)$, we analyze the situation at the time of observation $s < t_p$, when one of the nodes began broadcasting, what is the probability that the other (one or more) nodes at the time of the start of broadcasting. Of course, these probabilities are higher (at 10^{-5}) for the selected network parameters examined to illustrate the issue, which is obvious. In the range up to 50 nodes in the WSN the probability of signal disturbance from one node by another node begins broadcasting is linear. Comparing Fig. 2b and Fig. 3b we see that this increase is proportional, hence the practical application shows how to use the shortest communication protocols. This is an obvious application in the light of the objectives of the access network realization of a random result of previous work [15-17], which confirms the above analysis. Establishment of one-way transmission to the base station, the lack of communication between nodes (single-hop) allows a considerable shortening of the duration of the communication protocol (t_p), the header can be reduced to a maximum number of nodes defining the fields and define a

combination of starting. In practice this means that the correct transmission quality for this class of WSN network.

References

1. Pottie G.J. Wireless integrated network sensors / G.J. Pottie, W.J. Kaiser // Communications of the ACM. – 2000. – Vol.43, No.5. – PP. 51-58.
2. Culler D. Guest Editors' Introduction: Overview of Sensor Networks / D. Culler, D. Estrin, M. Srivastava // Computer. – 2004. – Vol.37, No.8. – PP. 41-49.
3. Perkins C.E. Ad Hoc Networking / C.E. Perkins. – Boston : Addison-Wesley, 2001. – 370 p.
4. Курітник І.П. Безпровідна трансляція інформації [Текст] / Ігор Петро Курітник, Микола Карпінський ; пер. з пол. магістра Володимира Карпінського та магістра Уляни Яциковської. – Т. : Крок, 2010. – 376 с. : рис.
5. Chatzigiannakis I. Efficient data propagation strategies in wireless sensor networks using a single mobile sink / I. Chatzigiannakis, A. Kinalis, S. Nikoletseas // Computer Communications. – 2008. – Vol. 31, Iss.5. – PP. 896-914.
6. Akyildiz I.F. Wireless sensor networks: a survey / I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci // Computer networks. – 2002. – Vol.38, Iss.4. – PP. 393-422.
7. Zorzi M. Error Control and Energy Consumption in Communications for Nomadic Computing / M. Zorzi, R.R. Rao // IEEE Transactions on Computers. – 1997. – Vol.46, No.3. – PP. 279-289.
8. Brzezinski A. Enabling Distributed Throughput Maximization in Wireless Mesh Networks: A Partitioning Approach / A. Brzezinski, G. Zussman, E. Modiano // MobiCom'06 Proceedings of the 12th annual international conference on Mobile computing and networking, September 23-26, 2006, Los Angeles, California, USA. – 2006. – PP. 26-37.
9. Shih E. Physical Layer Driven Algorithm and Protocol Design for Energy-Efficient Wireless Sensor Networks / E. Shih, S. Cho, N. Ickes, R. Min, and *et al.* // MobiCom'01 Proceedings of the 7th annual international conference on Mobile computing and networking, July 15-21, 2001, Rome, Italy. – 2001. – PP. 272-287.
10. Wattenhofer H. Algorithms for Wireless Sensor Networks (Tutorial) / H. Wattenhofer // Lecture Notes in Computer Science. – 2006. – Vol.3868. – P. 2.
11. Gupta P. The capacity of wireless networks / P. Gupta, P.R. Kumar // IEEE Transactions on Information Theory. – 2000. – Vol.46, Iss.2. – PP. 388-404.
12. Baccelli F. The role of PASTA in network measurement / F. Baccelli, S. Machiraju, D. Veitch, J. Bolot // ACM SIGCOMM Computer Communication Review – Proceedings of the 2006 conference on Applications, technologies, architectures, and protocols for computer communications, October 2006. – 2006. – Vol.36, Iss.4. – PP. 231-242.
13. Baccelli F. On Optimal Probing for Delay and Loss Measurement / F. Baccelli, S. Machiraju, D. Veitch, J. Bolot // Proceedings 2007 ACM SIGCOMM Internet Measurement Conference, San Diego, California, October 2007. – 2007. – PP. 291-302.
14. Feller W. Wstęp do rachunku prawdopodobieństwa / W. Feller, R. Bartoszyński, B. Bielecki // Warszawa: Państwowe Wydawnictwo Naukowe, 2006. – 456 p.
15. Rajba S. Wireless sensor convergecast based on random operations procedure / S. Rajba, T. Rajba // Pomiary, Automatyka, Kontrola. – 2010. – R. 56, Nr. 3. – PP. 255-258.
16. Rajba S. Wireless sensor network with random sending / S. Rajba, T. Rajba // Knowledge in Telecommunication Technologies and Optics: Proceedings of the 11th International Conference : KTTO 2011 : June 22-24, 2011, Szczyrk, Poland. – 2011. – PP. 170-175.
17. Rajba S. The probability of collisions in Wireless Sensor Network with random sending / S. Rajba, T. Rajba // Przegląd Elektrotechniczny. – 2012. – Nr 9a. – PP. 243-246.

ВИПАДКОВЕ КЕРУВАННЯ ПОСИЛАННЯМ РАДІОПОВІДОМЛЕНЬ В БЕЗПРОВІДНІЙ СЕНСОРНІЙ МЕРЕЖІ

С.В. Райба

University of Bielsko-Biala,
ul. Willowa, 2, 43-309 Bielsko-Biala, Poland; e-mail: rajbas@ath.bielsko.pl

У роботі наведено метод передавання з випадковим керуванням в безпровідній сенсорній мережі (БСМ). Встановлено умови, що є імовірністю стану без колізій БСМ-мережевого передавання одновузлового типу. Наукова новизна даної роботи полягає в концепції БСМ з випадковим одностороннім передаванням сигналів, використовуючи одну радіочастоту. Керування доступом до мережі здійснюється за допомогою використання PASTA (Пуассонівське надходження викликів, спостережуване за середній час) для моделювання БСМ. Визначено як імовірність колізій на інтервалі заданої малої довжини, так і імовірність вихідної кількості часових повідомлень у вузлах, які знаходяться в колізії під час передавання.
Ключові слова: безпровідна сенсорна мережа, PASTA, імовірність колізії, випадкове керування

СЛУЧАЙНОЕ УПРАВЛЕНИЕ ПЕРЕДАЧЕЙ РАДИОСООБЩЕНИЙ В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ

С.В. Райба

University of Bielsko-Biala,
ul. Willowa, 2, 43-309 Bielsko-Biala, Poland; e-mail: rajbas@ath.bielsko.pl

В работе приведен метод передачи со случайным управлением в беспроводной сенсорной сети (БСС). Установлены условия, являющиеся вероятностью состояния без коллизий БСС-сетевой передачи одноузлового типа. Научная новизна данной работы заключается в концепции БСС со случайной односторонней передачей сигналов с использованием одной радиочастоты. Управление доступом к сети осуществляется путем использования Poisson Arrivals See Time Averages (Пуассоновское поступление вызовов, наблюдаемое за среднее время) для моделирования БСС. Определены как вероятность коллизий на интервале заданной малой длины, так и вероятность исходного количества временных сообщений в узлах, которые находятся в коллизии при передаче.
Ключевые слова: беспроводная сенсорная сеть, PASTA, вероятность коллизии, случайное управление

УДК 621.382

Informatics and Mathematical Methods in Simulation
Vol. 2 (2012), No. 2, pp. 121-128

ПОВЫШЕНИЕ ПОМЕХОУСТОЙЧИВОСТИ ПРОЦЕДУРЫ КЛАССИФИКАЦИИ ПРИ КОНТРОЛЕ КАЧЕСТВА ШАБЛОНОВ

Ю.Ю. Козина

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: yuliyakc@mail.ru

В работе предложен помехоустойчивый метод классификации с обучением в пространстве гиперболического вейвлет-преобразования. В целях применения гиперболического вейвлет-преобразования к обработке изображений получено его дискретное представление. Изображение рассматривается как двумерная матрица с дискретными отсчетами.

Ключевые слова: гиперболическое вейвлет-преобразование, помехоустойчивость, шаблон, матрица

Введение

На современном этапе производства изделий микроэлектроники возникла потребность в производстве мелких и средних партий (около 50 тыс. в месяц), предназначенных для использования в аппаратуре специального назначения [1]. Контроль качества изделий микроэлектроники осуществляется с помощью программно-аппаратных комплексов (ПАК), включающих подсистемы формирования, регистрации и распознавания изображений. При этом используются сложные и дорогостоящие осветительно-фокусирующие устройства (ОФУ), телевизионные датчики (ТД) высокого разрешения и устройства точной механики, обеспечивающие высокие производительность и достоверность контроля качества шаблонов (носителей информации про размеры и конфигурацию изделий микроэлектроники). Стоимость таких комплексов составляет в среднем 100 тыс. у.е. за единицу. В таких условиях применение существующих ПАК приводит к неоправданному росту стоимости процесса контроля качества шаблонов. Таким образом, существует противоречие между высокой стоимостью систем контроля, предназначенных для массового производства, и необходимостью производства мелких и средних партий изделий. Это противоречие может быть разрешено снижением требований к ОФУ, ТД и устройствам точной механики. Однако, снижение требований к ОФУ приводит к неравномерной освещенности шаблонов и, следовательно, к появлению мультипликативных помех, а снижение требований к ТД приводит к появлению аддитивных помех. В условиях помех со значениями отношения сигнал/шум для аддитивной помехи 8..11 (по мощности) и 7..10 для мультипликативной помехи (по мощности) существующие ПАК не работоспособны. Кроме того, малые объемы обучающей выборки, характерные для мелкосерийного производства изделий, также уменьшают достоверность распознавания изображений, а, следовательно, и достоверность контроля качества шаблонов. Для решения этой научно-практической задачи необходимо разрабатывать системы, обеспечивающие высокую достоверность контроля качества шаблонов в условиях помех и малых обучающих выборок. В настоящее время таковыми являются системы искусственного интеллекта (СИИ) [2-5].

Цель статьи и постановка задания

При реализации СИИ для контроля качества шаблонов выполняется ряд процедур. Выявлено, что основным источником помех при этом являются процедуры локализации и классификации реперных знаков (РЗ) [6].

Реперные знаки – это объекты известной формы, которые наносятся на поверхность шаблона и используются для позиционирования шаблонов относительно друг друга. Процедура локализации РЗ предусматривает определение координат их местоположения на изображении шаблона. Процедура классификации РЗ предусматривает определение класса, к которому он принадлежит. Эти процедуры должны быть реализованы с высокой точностью и помехоустойчивостью.

При позиционировании шаблонов по РЗ их локализация, выделение и прослеживание контуров реализуется в пространстве гиперболического вейвлет-преобразования (ГВП) [7]. Идентификация осуществляется на базе структурно-статистического метода по характерным точкам контура РЗ [8]. После проведения процедуры локализации и идентификации выполняется процедура классификации в признаковом пространстве.

Среди классических методов реализации алгоритмов классификации выделяют градиентный метод, в частности метод градиентного спуска (ГС) [9]. Градиентные методы обладают рядом недостатков: чувствительность к начальной точке поиска, в условиях шумов оценка градиента затруднена и направление поиска выбирается неверно.

Целью работы является разработка помехоустойчивого метода классификации с обучением в пространстве ГВП.

Основная часть

В работе предложен помехоустойчивый метод классификации с обучением в пространстве ГВП. В целях применения ГВП к обработке изображений получено его дискретное представление. В данном случае изображение рассматривается как двумерная матрица с дискретными отсчетами. Строка либо столбец изображения рассматривается как дискретная последовательность $\{z_c\}$. ГВП некоторой дискретной последовательности $\{z_c\}$ определяется как свертка этой последовательности с базисной функцией $\Omega(\tau)$, которая соответствующим образом перенормируется с масштабом s (длина носителя гиперболического вейвлет-фильтра) и сдвигается по пространственной шкале на интервал $c\Delta\tau$:

$$WH(c,s) = \sum_{c'=0}^{C-1} z_c \Omega^* \left(\frac{(c'-c)\Delta\tau}{s} \right), \qquad (1)$$

где C – длина дискретной последовательности $\{z_c\}$.

Помехоустойчивый метод классификации реализован на основе субградиентного итеративного поиска экстремумов в пространстве ГВП. При его реализации выполняются следующие шаги:

Шаг 1. Определяются эмпирически длина носителя s и шаг итерации ϕ.

Шаг 2. Задается начальное приближение поиска минимума функционала качества $F(\mathbf{x},\mathbf{w})$, где $\mathbf{x}$ – вектор случайных возмущений; $\mathbf{w} = (w_1, w_2, ...w_n)$ – вектор настраиваемых параметров.

Шаг 3. С помощью пробного изменения в обоих направлениях от начального приближения с интервалом Δ, в зависимости от длины носителя s строятся

разделяющие поверхности (РП) и вычисляется функция ошибок $ES(\mathbf{w},i)$ при пробном изменении (рис. 1):

$$\mathbf{w}_i=\mathbf{w}_0\pm\Delta, \tag{2}$$

где

$i=\overline{1,s}$;

$\Delta=\dfrac{\mu_1-\mu_2}{4}$ – интервал изменения $\mathbf{w}_0$;

$(\mu_1-\mu_2)$ – расстояние между центрами классов.

Шаг 4. Вычисляется свертка функции ошибок $ES(\mathbf{w},i)$, полученной при пробном изменении, с функцией $\Omega(i)$:

$$\mathbf{HK}(\mathbf{w})=\frac{1}{s}\sum_{i=1}^{s}ES(\mathbf{w},i)\cdot\Omega(i). \tag{3}$$

Шаг 5. Определяется точка минимума функционала качества $F(\mathbf{x},\mathbf{w})$ в соответствии с:

$$\mathbf{w}[k+1]=\mathbf{w}[k]+\phi[k]\mathbf{HK}(\mathbf{w}[k]),\quad k=0,1,2,\ldots,K, \tag{4}$$

где

ϕ – шаг итерации;

$\mathbf{HK}(\mathbf{w}[k])$ – оценка субградиента в точке $\mathbf{w}[k]$ по (3);

K – определяется условиями останова алгоритма поиска минимума $F(\mathbf{x},\mathbf{w})$.

Условием останова алгоритма поиска минимума функционала $F(\mathbf{x},\mathbf{w})$ является изменение знака свертки ГВП (рис. 2). Выбрана длина носителя $s=17$, при котором алгоритм (4) повышает вероятность выхода в область глобального минимума функционала качества $F(\mathbf{x},\mathbf{w})$.

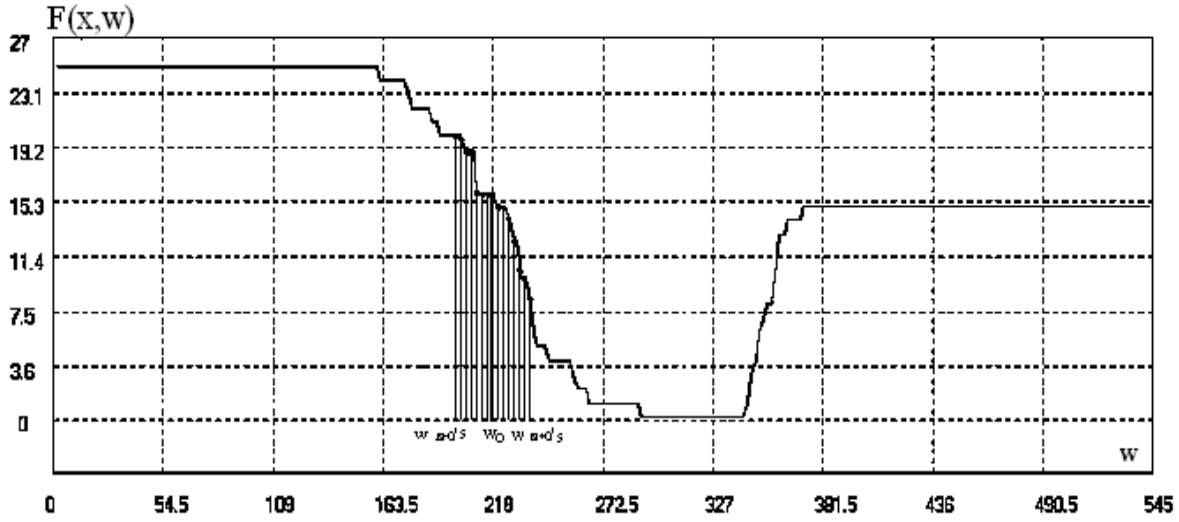


Рис. 1. Вычисление функции ошибок $ES(\mathbf{w},i)$ при пробных приращениях

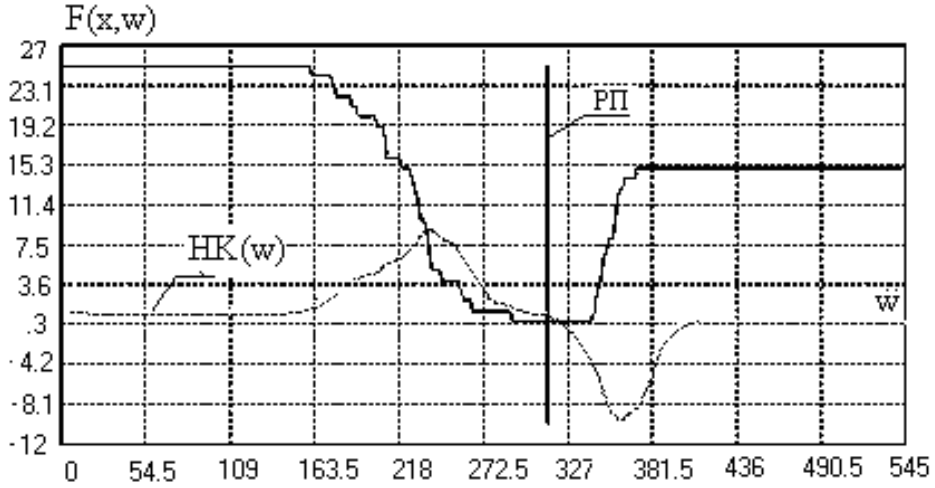


Рис. 2. Поиск минимума функционала качества $F(\mathbf{x},\mathbf{w})$

В целях определения шага итерации ϕ проведены исследования скорости сходимости алгоритма (4) при различных длинах носителя s и отношениях сигнал/шум q по мощности (рис. 3).

На основании приведенных зависимостей, например для $q=8$, рекомендован выбор шага итерации ϕ для каждого s: при $s_1=6$ – $\phi=\Delta/6$; при $s_2=17$ – $\phi=\Delta/15$; $s_3=30$ – $\phi=\Delta/21$.

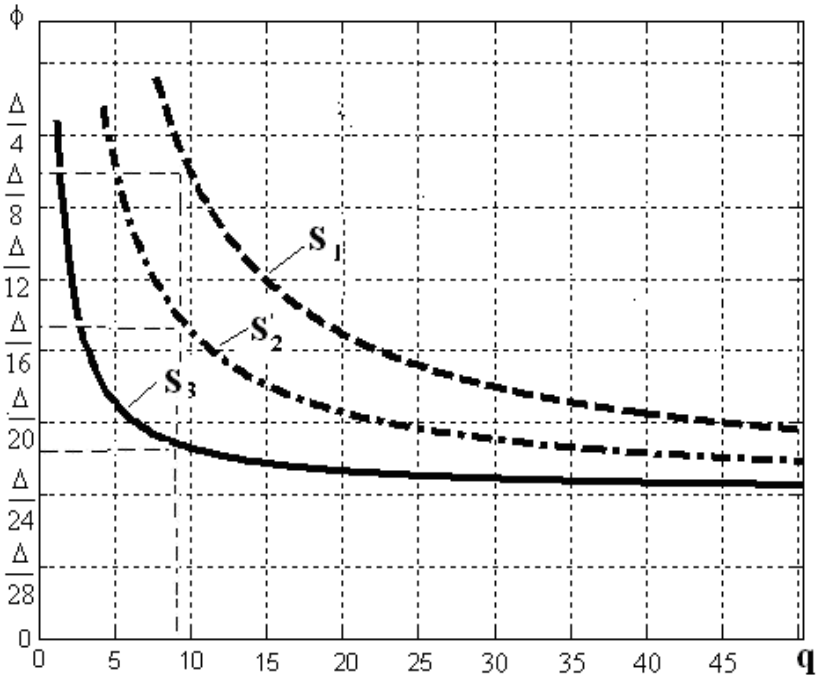


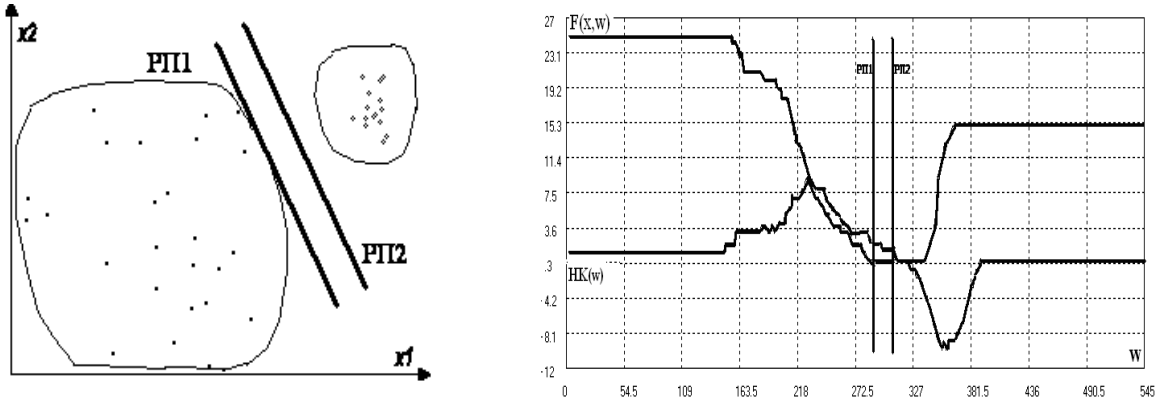
Рис. 3. Зависимость шага итерации ϕ от отношения сигнал/шум q по мощности при различных значениях длины носителя s $(s_1<s_2<s_3)$

Выполнен сравнительный анализ результатов применения метода ГС и метода на основе ГВП. Для этого в работе этими методами построены РП в двумерном прост-

ранстве признаков x_1, x_2 и выполнен поиск минимума функционала $F(\mathbf{x},\mathbf{w})$ для непересекающихся, близко расположенных и пересекающихся кластеров РЗ. Рассматривается случай двух классов. На рис. 4 представлен результат построения РП и поиска минимума $F(\mathbf{x},\mathbf{w})$ для непересекающихся классов методом ГС (РП1) и методом на основе ГВП (РП2) ($s=17$).

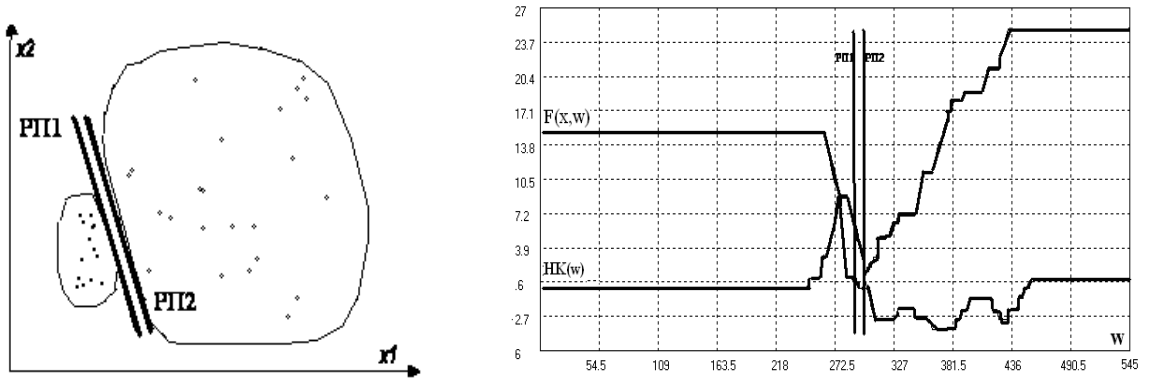
Как видно из рис. 4, алгоритм поиска на основе метода ГС, позволил выйти в область глобального минимума, но остановился в относительной близости к ошибке. Это связано с тем, что направление движения к минимуму функционала $F(\mathbf{x},\mathbf{w})$ определяется с точностью до знака направления градиента. Критерием завершения поиска будет выход на прямолинейный участок функционала $F(\mathbf{x},\mathbf{w})$, т.е. $\partial F/\partial w = 0$.

При построении РП для близко расположенных (рис. 5) и пересекающихся кластеров РЗ (рис. 6) методом ГС получим ошибку, за счет остановки в локальном минимуме $F(\mathbf{x},\mathbf{w})$. Применение разработанного метода на основе ГВП в данных случаях позволило повысить вероятность достижения области глобального минимума.



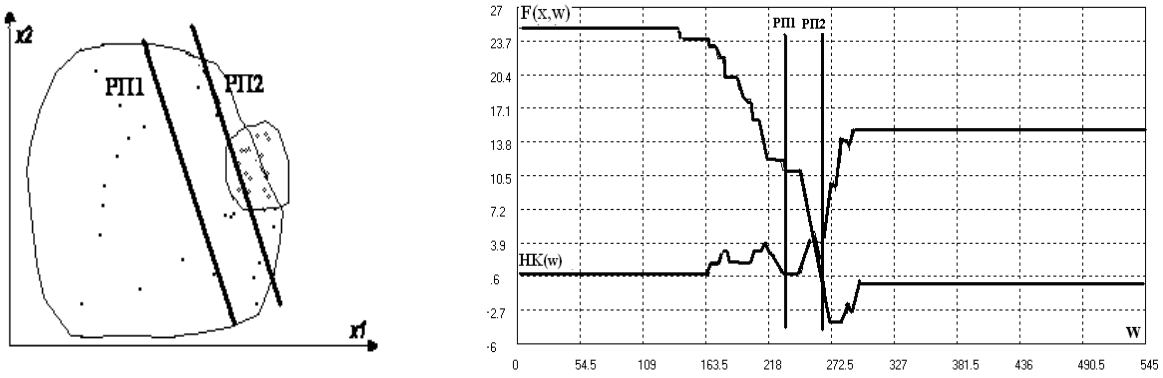
а **б**

Рис. 4. Построение РП и поиск минимума $F(\mathbf{x},\mathbf{w})$ для непересекающихся кластеров: кластеры РЗ в двумерном пространстве признаков (а); графики изменения $F(\mathbf{x},\mathbf{w})$ и $\mathbf{НК}(\mathbf{w})$ (б)



а **б**

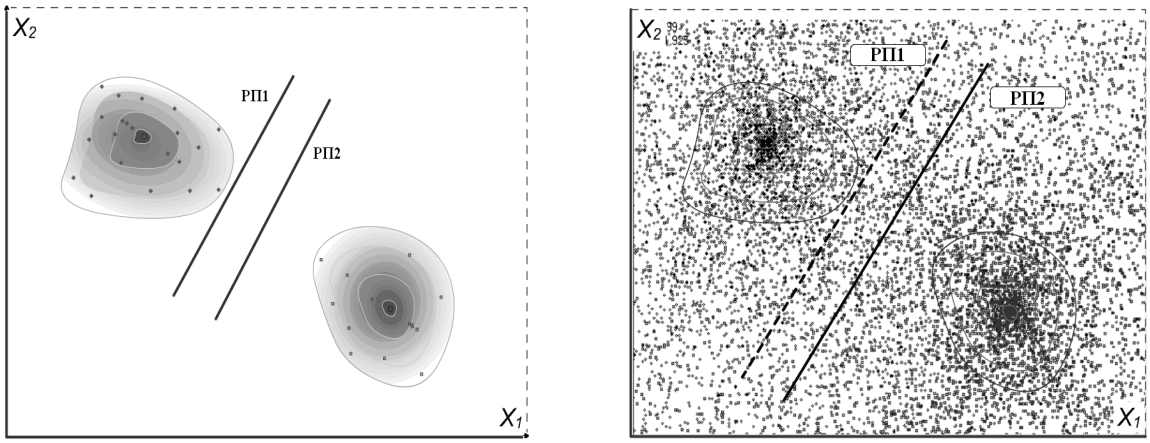
Рис. 5. Построение РП и поиск минимума $F(\mathbf{x},\mathbf{w})$ для близко расположенных классов: кластеры РЗ в двумерном пространстве признаков (а); графики изменения функций $F(\mathbf{x},\mathbf{w})$ и $\mathbf{НК}(\mathbf{w})$ (б)



а **б**

Рис. 6. Построение РП и поиск минимума $F(\mathbf{x},\mathbf{w})$ для пересекающихся классов: кластеры РЗ в двумерном пространстве признаков (а); графики изменения функций $F(\mathbf{x},\mathbf{w})$ и $\mathbf{HK}(\mathbf{w})$ (б)

Для исследования помехоустойчивости разработанного метода классификации создана модель ситуации изменения шумов (рис. 7). Данная ситуация может сложиться в условиях малого объема обучающей выборки и изменяющейся во время технологического процесса дисперсии кластеров РЗ.



а **б**

Рис. 7. Моделирование ситуации изменения шумов: режим обучения – построение РП (а); рабочий режим – классификация образов РЗ относительно РП (б)

В этих условиях выполнена классификация образов РЗ в рабочем режиме. Получены оценки зависимости изменения суммарной вероятности ошибок первого и второго рода P от среднеквадратического отклонения g, которое представляет собой численную характеристику разброса образов РЗ относительно центра кластера (рис. 8). При этом предложено определить g так:

$$g = \frac{g_{\text{г}}}{g_0}, \qquad (5)$$

где

g_r – среднеквадратическое отклонение рабочего режима;

g_0 – среднеквадратическое отклонение режима обучения.

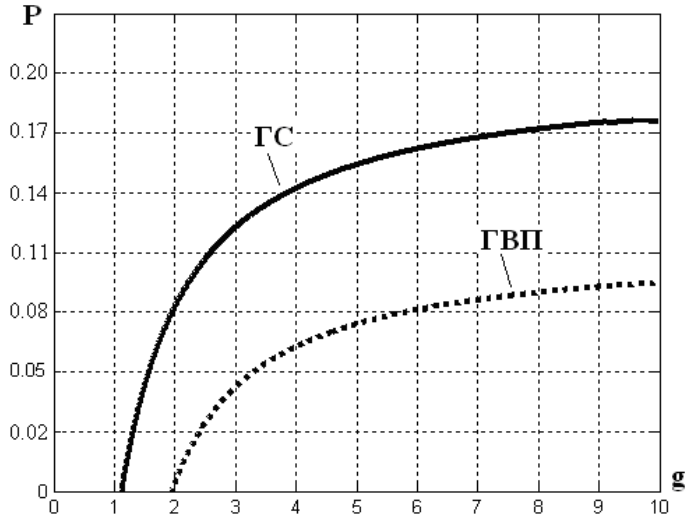


Рис. 8. Зависимость изменения суммарной вероятности ошибок первого и второго рода P от среднеквадратического отклонения g

Заключение

Эксперименты показали, что в результате применения разработанного метода классификации суммарная вероятность ошибок первого и второго рода уменьшилась до 1.5 раз по сравнению с методов ГС, при изменении среднеквадратического отклонения от 1 до 10 в пространстве признаков. На основании этого можно сделать вывод о повышении помехоустойчивости процедуры классификации РЗ в условиях помех и малых объемах обучающей выборки.

Список литературы

1. Задорин А.Ю. Система автоматизированного визуального контроля печатных плат Aplite / А.Ю. Задорин, Г.Б. Захарова // Chip News. Инженерная микроэлектроника. – 2002. – № 10. – С. 53-56.
2. Уинстон П.Г. Искусственный интеллект [Текст] / П.Г. Уинстон; пер. В.Л. Стефанюк, ред. Д.А. Поспелов. – М. : Мир, 1980. – 519 с.
3. Люггер Д.Ф. Искусственный интеллект. Стратегии и методы решения сложных проблем [Текст] / Д.Ф. Люгер ; пер. с англ. Н.И. Галаган [и др.]. – М. ; СПб. ; К. : Издательский дом «Вильямс», 2005. – 863 с.: рис.
4. Распознавание образов [Текст] : состояние и перспективы / К. Верхаген, Р. Дёйн, Ф. Грун и др.; Пер. с англ. Н.Г. Гуревич, Под ред. И.Б. Гуревича. – М. : Радио и связь, 1985. – 103 с. : ил.
5. Бондарев В.Н. Искусственный интеллект [Текст] : Учеб. пособие для студ. вузов / В.Н. Бондарев, Ф.Г. Аде. – Севастополь : Издательство СевНТУ, 2002. – 615 с.
6. Гаршин В. Автоматы установки компонентов серии X^{II} / В. Гаршин, Г. Егоров // Электроника: Наука, Технология, Бизнес. – 2004. – № 5. – С. 16-18.
7. Антощук С.Г. Обработка изображений в области гиперболического вейвлет-преобразования / С.Г. Антощук, В.Н. Крылов // Автоматика. Автоматизация. Электротехнические комплексы и системы. – 2003. – № 2(12). – С. 7-10.

8. Щербакова Г.Ю. Идентификация изображений реперных знаков в системах АОК ИЭТ / Г.Ю. Щербакова, В.Н. Крылов, Ю.Ю. Козина// Труды Седьмой междунар. науч.-практ. конф. «Современные информационные и электронные технологи» (СИЭТ-2006), 22 – 26 мая 2006 г., Одесса, Украина. – Одесса: ВМВ. – 2006. – С. 67.
9. Гонсалес Р. Цифровая обработка изображений [Текст] : пер. с англ. / Р.С. Гонсалес, Р.Э. Вудс ; ред. пер. ЧоП. А. Чочиа. – М. : Техносфера, 2006. – 1070 с.

ПІДВИЩЕННЯ ЗАВАДОСТІЙКОСТІ ПРОЦЕДУРИ КЛАСИФІКАЦІЇ ПРИ КОНТРОЛІ ЯКОСТІ ШАБЛОНІВ

Ю.Ю. Козіна

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: yuliyakc@mail.ru

У роботі запропоновано завадостійкий метод класифікації з навчанням в просторі гіперболічного вейвлет-перетворення. З метою застосування гіперболічного вейвлет-перетворення до обробки зображень отримано його дискретне представлення. Зображення розглядається як двовимірна матриця з дискретними відліками.
Ключові слова: гіперболічне вейвлет-перетворення, завадостійкість, шаблон, матриця

NOISE STABILITY INCREASE OF CLASSIFICATION PROCEDURE UNDER QUALITY CONTROL OF TEMPLATES

Yuliya Yu. Kozina

Odessa National Polytechnic University,
1 Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: yuliyakc@mail.ru

In current article noise stability classification method of training in hyperbolic wavelet transformation space is suggested. For purposes of applying of hyperbolic wavelet transformation to image processing, its discreet representation is received. An image is considered as two-dimensional matrix with discreet counting.
Keywords: hyperbolic wavelet transformation, noise stability, template, matrix

Mathematics Subject Classification (2010) 97M50

Informatics and Mathematical Methods in Simulation
Vol. 2 (2012), No. 2, pp. 129-133

FEATURES OF DENIAL-OF-SERVICE ATTACKS IN INFORMATION SYSTEMS

Marek A. Aleksander[1], Mikolaj P. Karpinski[2], Uliana O. Yatsykovska[3]

[1] State Higher Vocational School in Nowy Sacz,
ul. Zamenhofa, 1a, 33-300 Nowy Sacz, Poland; e-mail: aleksmar@pwsz-ns.edu.pl
[2] University of Bielsko-Biala,
ul. Willowa, 2, 43-309 Bielsko-Biala, Poland; e-mail: mkarpinski@ath.bielsko.pl
[3] Ternopil Ivan Pul'uj National Technical University,
56 Ruska str., Ternopil, 46001, Ukraine; e-mail: price@ukr.net

The paper proposes a mathematical model of communication of client-server that includes the probability of compromised node and the number of all possible routes that can have an admission to access points, have done a comparative characteristics of attacks DoS / DDoS in information systems.

Keywords: computer network, denial of service, mathematical model

Introduction

Because the principle of open networks and access to them are specific features of their structure and processes of operation, such as openness, protection [1], characterized by significant heterogeneity [2]. At present, special attention focuses on new areas of development and improvement of data networks. Among them should provide wireless (mobile) networks. Such networks provide the user with unique opportunities for fast access to remote network resources, including the global network Internet, limiting his mobility, not linking to the wired communication lines [3].

With the development and complication of the tools, techniques and processes of information processing increases dependence of modern society on the degree of security used his information technology [4].

Computer network providing every opportunity for exchanging data between the client and server, but now widely distributed attack denial of service clients, the determination of distributed attacks in the network is particularly acute. The most common types of such attacks are DoS / DDoS attacks, which deny certain users of computer network services.

With the constant development of computer networks and the increasing number of users grows and the number of new types of attacks to denial of service. DoS / DDoS attacks are characterized by a straightforward implementation complexity and resistance, which poses new problems of researchers, who are still not yet resolved. Analysis of recent publications shows that exercise is accompanied by attacks: interception of confidential information to unauthorized use of network bandwidth and computational resources, the spread of false information, violation of network administration.

The main part

To solve the task should use the classification of information threats, DoS / DDoS attacks and formalized models [1] measure the impact on job performance computer network.

This will effectively solve the problem of detecting attacks on computer network access point. Construct formal mathematical models of probability of information threats, DoS / DDoS attacks based on the linear form of the method of weighting coefficients.

$$P\_IT(P) = \alpha_1 P_{\text{Confidentiality}} + \alpha_2 P_{\text{Integrity}} + \alpha_3 P_{\text{Accessibility}}, \quad (1)$$

$$P\_DoS(P) = \beta_1 P_{Smurf} + \beta_2 P_{Fraggle} + \beta_3 P_{SYNFlood} + \beta_1 P_{DNS}, \quad (2)$$

$$P\_DDoS(P) = \delta_1 P_{Trinoo} + \delta_2 P_{TAN/TF2K} + \delta_3 P_{Stacheldraht}, \quad (3)$$

where

$P\_IT(P)$ – probability of information threats;

$P\_DoS(P)$ – probability of DoS attacks;

$P\_DDoS(P)$ – probability of DDoS attacks;

α_i – weighting coefficients, where $\alpha_i \in [0;1]$;

β_i – weighting coefficients, where $\beta_i \in [0;1]$;

δ_i – weighting coefficients, where $\delta_i \in [0;1]$.

The mathematical model defining the matrix network activity, according to which make conclusions about the realization of attack:

$$\alpha_{IT} = \begin{bmatrix} \alpha_1^a & \alpha_2^a & \alpha_3^a \\ \alpha_1^b & \alpha_2^b & \alpha_3^b \\ \alpha_1^c & \alpha_2^c & \alpha_3^c \\ \alpha_1^d & \alpha_2^d & \alpha_3^d \\ \alpha_1^e & \alpha_2^e & \alpha_3^e \\ \alpha_1^f & \alpha_2^f & \alpha_3^f \\ \alpha_1^g & \alpha_2^g & \alpha g \end{bmatrix}, \ \beta_{DoS} = \begin{bmatrix} \beta_1^a & \beta_2^a & \beta_3^a & \beta_4^a \\ \beta_1^b & \beta_2^b & \beta_3^b & \beta_4^b \\ \beta_1^c & \beta_2^c & \beta_3^c & \beta_4^c \\ \beta_1^d & \beta_2^d & \beta_3^d & \beta_4^d \\ \beta_1^e & \beta_2^e & \beta_3^e & \beta_4^e \\ \beta_1^f & \beta_2^f & \beta_3^f & \beta_4^f \\ \beta_1^g & \beta_2^g & \beta_3^g & \beta_4^g \end{bmatrix},$$

$$\delta_{DDoS} = \begin{bmatrix} \delta_1^a & \delta_2^a & \delta_3^a \\ \delta_1^b & \delta_2^b & \delta_3^b \\ \delta_1^c & \delta_2^c & \delta_3^c \\ \delta_1^d & \delta_2^d & \delta_3^d \\ \delta_1^e & \delta_2^e & \delta_3^e \\ \delta_1^f & \delta_2^f & \delta_3^f \\ \delta_1^g & \delta_2^g & \delta_3^g \end{bmatrix} \quad (4)$$

The research has shown that all types of attacks evenly affecting computer network. With increasing probability kinds of attacks the probability of information threats and DoS/DDoS attack increases directly proportional. The denial of service attack has the greatest impact on network performance. But to discern what kind of attack is practically implemented, these models do not allow.

To determine the types of attack that is implemented, form the mathematical model of communication and customer service, which includes the likelihood compromise node and the number of ways to whatever they access points.

$$\text{I} \qquad \alpha_i^a = \frac{1}{k}\left[P_{AP}^1 + P_{AP}^2\right],$$

$$\text{II} \qquad \alpha_i^b = \frac{1}{k}\left[2P_{AP}^1 + P_{AP}^2\right],$$

$$\text{III} \qquad \alpha_i^c = \frac{1}{k}\left[P_{AP}^1 + 2P_{AP}^2\right],$$

$$\text{IV} \qquad \alpha_i^d = \frac{1}{k}\left[2P_{AP}^1 + 2P_{AP}^2\right], \qquad (5)$$

$$\text{V} \qquad \alpha_i^e = \frac{1}{k}\left[2P_{AP}^1 + P_{AP}^2\right],$$

$$\text{VI} \qquad \alpha_i^f = \frac{1}{k}\left[P_{AP}^1 + 2P_{AP}^2\right],$$

$$\text{VII} \qquad \alpha_i^g = \frac{1}{k}\left[P_{AP}^1 + P_{AP}^2\right],$$

where

$\alpha_i^{a,b,c,d,e,f,g}$ – weighting coefficient,

a, b, c, d, e, f, g – model of communication,

i – types of attacks,

k – number of possible paths from AP to T.

Here are the results of numerical experiment with the model (5) in graphic form (Fig. 1).

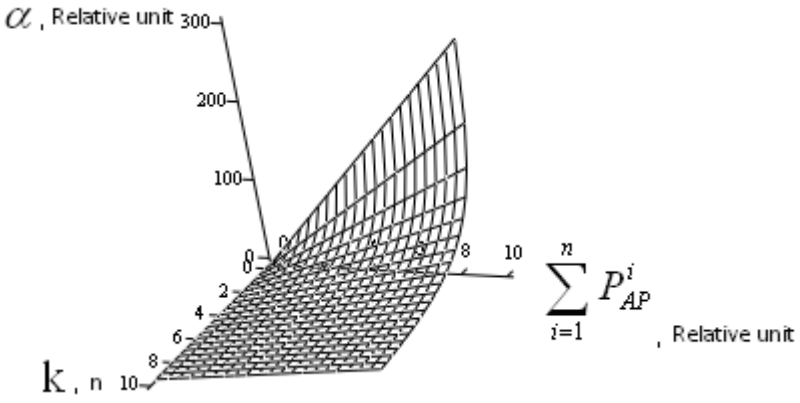


Fig. 1. Dependence of probability weights compromised access points, and number of whatever routs: α – weighting coefficient, n – number of nodes, $\sum_{i=1}^{n} P_{AP}^i$ – the total number of probably compromised access points

The research have shown that as the number of ways to whatever they can from client to server network activity is low, so the practical realization of attack is difficult to determine. For small values k, the active of network is growing rapidly, the attack is determined unambiguously. Level of the compromised nodes has a little impact on network activity in general, since these units do not determine the process routing.

To distinguish between that attacks was realized, we use Table 1 which analyzed the way to and through compromised node.

Table 1.

Comparative characteristics of attacks DoS/DDoS, computer network

Type of attack		Route, k			Passing through the compromised node
		min	indefinite	determined	
DoS	Smurf	–	+	–	–
	Fraggle	–	+	–	–
	SYN Flood	–	+	–	+
	DNS	–	–	+	–
DDoS	Trinoo	–	+	–	+
	TAN/TF2K	–	–	+	+
	Stacheldraht	–	+	–	+

It should be noted that the attacks and DNS TAN/TF2K implemented on a specific path, because in a computer network they are easy to detect by analyzing traffic. Traffic activity increases significantly in the implementation of such attacks. In other cases it is difficult to determine the type of threat.

Conclusions, recommendations and perspectives for future development of this area

Research have shown that the formal mathematical model of probability information of threats and DoS/DDoS attacks based on the linear form of the method of weighting coefficients do not allow to discern what kind of attack is practically implemented in a computer network, because with increasing probabilities of attack types increases directly proportional probability information of threats and attacks, DoS/DDoS.

Dependence of probability weights compromised access points and ways of whatever they have shown that for small values k active network is growing rapidly and clearly defined attack. When increasing the number of ways to whatever they can from the client to the server, practical realization of attack is difficult to determine because of the low activity of the network. Level nodes of compromise have a little impact on network activity in general, since these units do not determine the process routing.

References

1. Mylokum Y. Models and methods of providing services in secure computer networks (in Ukrainian): synopsis of PhD thesis, 05.13.05 «Computer Systems & Components» / Y. Mylokum; National Aviation University. – Kyiv, 2009. – 20 p.
2. Chang Shu. The method of adaptive formation of traffic flows at computer networks (in Ukrainian): synopsis of PhD thesis, 05.13.05 «Computer Systems & Components» / Chang Shu; National Aviation University. – Kyiv, 2009. – 20 p.

3. Kolesnyk O.B. Information technology and tools for adaptive network management in wireless LAN (in Ukrainian): synopsis of PhD thesis, 05.13.06 «Information technology» / O.B. Kolesnyk; Kharkiv National University of Radioelectronics. – Kharkiv, 2008. – 25 p.
4. Ayrapetyan R.A. Methods of software protecting against unauthorized access and malicious software (in Ukrainian): synopsis of PhD thesis, 05.13.21 «Information security systems» / R.A. Ayrapetyan; Odessa National Polytechnic University. – Odessa, 2009. – 18 p.

ОСОБЛИВОСТІ DOS-АТАК В ІНФОРМАЦІЙНИХ СИСТЕМАХ

М.А. Алєксандер[1], М.П. Карпінський[2], У.О. Яциковська[3]

[1] State Higher Vocational School in Nowy Sacz,
ul. Zamenhofa, 1a, 33-300 Nowy Sacz, Poland; e-mail: aleksmar@pwsz-ns.edu.pl
[2] University of Bielsko-Biala,
ul. Willowa, 2, 43-309 Bielsko-Biala, Poland; e-mail: mkarpinski@ath.bielsko.pl
[3] Тернопільський національний технічний університет імені Івана Пулюя,
вул. Руська, 56, Тернопіль, 46001, Україна; e-mail: price@ukr.net

Запропоновано математичну модель архітектури «клієнт-сервер», яка враховує ймовірність порушення функціонування мережного вузла і можливі маршрути, через які здійснюється доступ до точок доступу. Наведено порівняльний аналіз DoS/DDoS-атак в інформаційних системах.
Ключові слова: комп'ютерна мережа, атака на відмову в обслуговуванні, математична модель

ОСОБЕННОСТИ DOS-АТАК В ИНФОРМАЦИОННЫХ СИСТЕМАХ

М.А. Александер[1], Н.П. Карпинский[2], У.О. Яциковская[3]

[1] State Higher Vocational School in Nowy Sacz,
ul. Zamenhofa, 1a, 33-300 Nowy Sacz, Poland; e-mail: aleksmar@pwsz-ns.edu.pl
[2] University of Bielsko-Biala,
ul. Willowa, 2, 43-309 Bielsko-Biala, Poland; e-mail: mkarpinski@ath.bielsko.pl
[3] Тернопольский национальный технический университет имени Ивана Пулюя,
ул. Русская, 56, Тернополь, 46001, Украина; e-mail: price@ukr.net

Предложена математическая модель архитектуры «клиент-сервер», которая учитывает вероятность нарушение функционирования сетевого узла и возможные маршруты, через которые осуществляется доступ к точкам доступа. Сделан сравнительный анализ DoS/DDoS-атак в информационных системах.
Ключевые слова: компьютерная сеть, атака типа «отказ в обслуживании», математическая модель

Mathematics Subject Classification (2010) 74A10

Informatics and Mathematical Methods in Simulation
Vol. 2 (2012), No. 2, pp. 134-142

THE STRESS STATE OF THE CONTINUOUS RECTANGULAR PLATE

Stanislav T. Rogovskiy, Victor V. Reut

Odessa I.I.Mechnikov National University,
2 Dvoryanskaya str., Odessa, 65082, Ukraine; e-mail: reut@onu.edu.ua

The problems on the continuous plates with the intermediate bearers are often necessary at the calculations of the building structures and constructions' elements in the mechanical engineering. As it was shown in [1, 2], the problems on the calculations of the plate shells and the folded-plate constructions are reduced to such problems also. The works of many native and foreign scientists are devoted to the calculation of the plates' stress state. The review of these works one can find in [3-5]. In the proposed article with the help of the integral transformation method [6], and the method of the three moments [7] the influence function is constructed. That allows to consider the more intricate problems on the stress state of the folded-plate constructions. The calculations of the characteristic values (the reactions and the bending moments on the bearers) are shown.

Keywords: shell, deformation, stress state, bending moment

The problem statement

The problem on the stress state of the continuous rectangular hingedly supported plate ($a < x < b, -l_1 < y < l_2$) is considered. The plate is hingedly supported along the lines $x = a_k$, $a_k = a + kl$, $l = (b-a)/n$, $k = \overline{1,n-1}$ with the help of the $n-1$ fixed bearing. The concentrated force P is applied at the point with the coordinates (ξ, n), $\xi \in (a_m, a_{m+1})$. It is necessary to estimate the bending moments' values $M_x(a_k, y)$ and the bearers' moments $N(a_k, y)$, $k = \overline{0,n}$.

Such problem is reduced to the solving of the Sophie-Germen biharmonic equation for the plates' bending

$$\Delta^2 w(x,y) = P\delta(x-\xi, y-\eta),\ a < x < b,\ x \neq a_k,\ k = \overline{1,n-1},\ |y| < \infty. \tag{1}$$

The solution of it should satisfy the conditions of the rectangular hingedly supporting

$$\begin{gathered} x = a,b\ :\ w = 0,\ M_x = 0, \\ y = -l_1, l_2\ :\ w = 0,\ M_y = 0, \end{gathered} \tag{2}$$

and the conditions on the bearers

$$x = a_k,\ k = \overline{1,n-1}:\ w = 0,\ <\varphi_x> = 0,\ <M_x> = 0. \tag{3}$$

At that

$$N(a_k, y) = \langle V_x \rangle\big|_{x=a_k}, \tag{4}$$

where $\varphi_x(x,y)$ is the bending angle of the plate, $M_x(x,y)$, $M_y(x,y)$ are the bending moments, $V_x(x,y)$, $V_y(x,y)$ are the generalized lateral forces, which are connected with the point's by the known formulas:

$$\varphi_x = \frac{\partial w}{\partial x},$$

$$M_x = -D\left(\frac{\partial^2 w}{\partial x^2} + \nu\frac{\partial^2 w}{\partial y^2}\right),$$

$$M_y = -D\left(\frac{\partial^2 w}{\partial y^2} + \nu\frac{\partial^2 w}{\partial x^2}\right), \tag{5}$$

$$V_x = -D\left(\frac{\partial^3 w}{\partial x^3} + (2-\nu)\frac{\partial^3 w}{\partial x \partial y^2}\right),$$

$$V_y = -D\left(\frac{\partial^3 w}{\partial y^3} + (2-\nu)\frac{\partial^3 w}{\partial x^2 \partial y}\right).$$

D is the flexural rigidity of a plate $D = \frac{Eh^3}{12(1-\nu^2)}$, ν is the Poisson's coefficient, E is the modulus of elasticity, h is the plate's thickness.

We define as $\langle\langle F(x,y)\rangle\rangle$, following by [1],

$$x = a: \langle\langle F(x,y)\rangle\rangle = F(a-0, y) - F(a+0, y)$$

– is the function $F(x,y)$ jump through the line $x = a$.

The solution of the boundary problem (1)-(5) is searching with the help of the finite sin-Fourier transformation

$$w_\lambda(x) = \int_{-l_1}^{l_2} w(x,y)\sin\lambda(y+l_1)dy, \tag{6}$$

$$w(x,y) = \frac{1}{2\pi}\sum_{k=1}^{\infty} w_\lambda(x)\sin\lambda(y+l_1), \quad \lambda = \frac{\pi k}{2l} \tag{7}$$

As a result the problem is reduced to the one-dimensional discontinuous boundary problem [6, App. II, § 2, p.2] of the form

$$w_\lambda^{IV}(x) - 2\lambda^2 w_\lambda''(x) + \lambda^4 w_\lambda(x) = P\delta(x-\xi)\sin\lambda(\eta+l_1), \tag{8}$$

$$w_\lambda\big|_{x=a,b} = 0, \quad w_\lambda''\big|_{x=a,b} = 0, \tag{9}$$

$$w_\lambda\Big|_{x=a_k}=0,\quad \langle w'_\lambda\rangle\Big|_{x=a_k}=0,\quad \langle w''_\lambda\rangle\Big|_{x=a_k}=0,\quad k=\overline{1,n-1}. \tag{10}$$

If the solution of this problem will be constructed, then with the help of the inverse Fourier transformation (7) one can obtain the solution of the stated problem in the form of a series.

The Green's function of the continuous problem

For the boundary problem (8, 9) solving, let's construct the Green's function $g_\lambda(x,\xi)$ of the tentative problem

$$L^2 w_\lambda = P\delta(x-\xi)\sin\lambda(\eta+l_1),\quad 0<x<l, \tag{11}$$

$$w_\lambda\Big|_{x=0,l}=0,\quad Lw_\lambda\Big|_{x=0,l}=0, \tag{12}$$

where $Lu=\partial^2 u/\partial x^2-\lambda^2 u$.

As it known [6, App. II, §1, p. 2, formula 1.17], the Green's function $g_\lambda(x,\xi)$ has the form:

$$g_\lambda(x,\xi)=\Phi_\lambda(x,\xi)-\sum_{j=0}^{3}c_i(\xi)\psi_j(x), \tag{13}$$

where $\Phi_\lambda(x,\xi)$ is the fundamental function of the equation (11), $\{\psi_j(x)\}_{j=0}^3$ is the fundamental basic system of the problem (11) – (12) solutions.

At that, the fundamental function of the equation (11) has the form [6, App. II, §1, p. 3, formula 1.34-35]

$$\Phi_\lambda(x,\xi)=\frac{1+\lambda|x-\xi|}{4\lambda^3}e^{-\lambda|x-\xi|}-\frac{1+\lambda(x+\xi)}{4\lambda^3}e^{-\lambda(x+\xi)}. \tag{14}$$

One can input the boundary functionals of the following form

$$U_0[u]=u\big|_{x=0},\quad U_1[u]=Lu\big|_{x=0},\quad U_2[u]=u\big|_{x=l},\quad U_3[u]=Lu\big|_{x=l}.$$

Then, the coefficients $c_i(\xi)$, $i=\overline{0,3}$ can be estimated as

$$c_i(\xi)=U_i[\Phi_\lambda],\quad i=\overline{0,3}. \tag{15}$$

and the elements of the fundamental basic system of the solutions can be found as the solutions of the corresponded problems

$$\begin{cases} L^2\psi_i=0 \\ U_j[\psi_j]=\delta_{ij} \end{cases},\qquad j=\overline{0,3},\quad i=\overline{0,3}, \tag{16}$$

where δ_{ij} is the Kronecker symbol.

So, with the help of (15) and (16), one obtain

$$c_0(\xi)=0, \quad c_1(\xi)=0,$$

$$c_2(\xi)=\frac{1}{2\lambda^3}e^{-\lambda l}\left((1+\lambda l)\mathrm{sh}\lambda\xi-\lambda\xi\mathrm{ch}\lambda\xi\right), \tag{17}$$

$$c_3(\xi)=-\frac{1}{\lambda}e^{-\lambda l}\mathrm{sh}\lambda\xi\,.$$

$$\psi_0(x)=\frac{\mathrm{sh}\lambda(l-x)}{\mathrm{sh}\lambda l}, \quad \psi_1(x)=\frac{\mathrm{sh}\lambda x}{\mathrm{sh}\lambda l},$$

$$\psi_2(x)=-\frac{l\mathrm{ch}\lambda l}{2\lambda\mathrm{sh}^2\lambda l}sh\lambda(l-x)+\frac{(l-x)\mathrm{ch}\lambda(l-x)}{2\lambda\mathrm{sh}l}, \tag{18}$$

$$\psi_3(x)=-\frac{l\mathrm{ch}\lambda l}{2\lambda\mathrm{sh}^2\lambda l}sh\lambda x+\frac{x\mathrm{ch}\lambda x}{2\lambda\mathrm{sh}\lambda l}.$$

The Green's function of the problem (11)-(12) one can construct after the substitution of the (17) and (18) in (13).

The form of the Green's function will be

$$G_\lambda(x,\xi)=n^3 g_\lambda\left((x-a)/n,(\xi-a)/n\right).$$

The Green's function of the discontinuous solution

It is necessary to construct the Green's function of the discontinuous boundary problem (8)-(9).

In the designations of the previous part this problem will be the following

$$L^2 w_\lambda = P\delta(x-\xi)\sin\lambda(\eta+l_1), \tag{19}$$

$$w_\lambda\big|_{x=a,b}=0, \quad Lw_\lambda\big|_{x=a,b}=0, \tag{20}$$

$$w_\lambda\big|_{x=a_k}=0, \quad \langle w'_\lambda\rangle\big|_{x=a_k}=0, \quad \langle Lw_\lambda\rangle\big|_{x=a_k}=0, \quad k=\overline{1,n-1}, \tag{21}$$

The Green's function of the discontinuous problem (19)-(21) has the form [6, App. II, §2, p. 2, formula 2.19]:

$$G^*_\lambda(x,\xi)=G_\lambda(x,\xi)-\sum_{k=1}^{n-1}\mu_k G_\lambda(x,a_k), \tag{22}$$

where

$$G_\lambda(x,\xi)=\Phi_\lambda(x,\xi)-\sum_{j=0}^{3}c_j(\xi)\psi_j(x)$$

is the Green's function of the continuous problem (is constructed in the previous part), $\mu_k=N_\lambda(a_k)$.

According the three moments' theorem [7, part XVII, § 248], instead the problem (19)-(21) let's consider the $n-1$ problems of the form

$$L^2w_\lambda=r_\lambda(x),\quad a_k<x<a_{k+1},$$

$$w_\lambda\big|_{x=a_k}=0,\quad w_\lambda\big|_{x=a_{k+1}}=0, \tag{23}$$

$$Lw_\lambda\big|_{x=a_k}=M_k,\quad Lw_\lambda\big|_{x=a_{k+1}}=M_{k+1},$$

where

$$r_\lambda(x)=\begin{cases}0, & a_k<x<a_{k+1}\\ f\delta(x-\xi), & a_m<x<a_{m+1}\end{cases}, \tag{24}$$

$$k\neq m,$$

at that $f=P\sin\lambda(\eta+l_1)$, M_k, $k=\overline{0,n}$ the transformations of the bending moments on the bearers are the unknown constants which are estimated from the second condition from (21).

$$w'_\lambda(a_k-0)=w'_\lambda(a_k+0),\quad k=\overline{1,n-1}. \tag{25}$$

The solution of the boundary problem (19)-(21), according [8], satisfies to the following correlation

$$w_\lambda(x)=\int_{a_k}^{a_{k+1}}r_\lambda(\xi)g_\lambda(x-a_k,\xi-a_k)d\xi-M_k\frac{\partial g_\lambda}{\partial\xi}(x-a_k,0)+M_{k+1}\frac{\partial g_\lambda}{\partial\xi}(x-a_k,l),$$

$$k=\overline{0,n-1}.$$

Then, with regard of the applied loading form (24), one obtain that on the each segment $a_k<x<a_{k+1}$, $k=\overline{0,n-1}$ the deflection's transformation $w_\lambda(x)$ should satisfy to ratio

$$w_\lambda(x)=\begin{cases}-M_m\dfrac{\partial g_\lambda}{\partial\xi}(x-a_m,0)+M_{m+1}\dfrac{\partial g_\lambda}{\partial\xi}(x-a_m,l)+fg_\lambda(x-a_m,\xi-a_m)\\ \qquad -M_k\dfrac{\partial g_\lambda}{\partial\xi}(x-a_k,0)+M_{k+1}\dfrac{\partial g_\lambda}{\partial\xi}(x-a_k,l)\end{cases}, \tag{26}$$

where $a_m<x<a_{m+1}$, $a_k<x<a_{k+1}$, $k=\overline{0,n-1}$, $k\neq m$.

One obtain the following equation for M_k because of the conditions (25):

$$TM_{k+1} - 2BM_k + TM_{k-1} = \begin{cases} 0, & 1 \le k \le m-1 \;\&\; m+1 \le k \le n-1 \\ f\dfrac{\partial}{\partial x} g_\lambda(0, \xi - a_m), & k = m \\ f\dfrac{\partial}{\partial x} g_\lambda(l, \xi - a_m), & k = m+1 \end{cases}, \tag{27}$$

here $M_0 = 0$, $M_n = 0$ in accordance with the condition (20),

$$T = -\frac{l\mathrm{ch}\lambda l}{2\mathrm{sh}^2 \lambda l} + \frac{1}{2\lambda \mathrm{sh}\lambda l},$$

$$B = \frac{l\mathrm{ch}^2 \lambda l}{2\mathrm{sh}^2 \lambda l} - \frac{\mathrm{ch}\lambda l + \lambda l \mathrm{sh}\lambda l}{2\lambda \mathrm{sh}\lambda l}.$$

The solution of the homogeneous system (27) one can search [7] in the form

$$M_k = Cq_1^k + Dq_2^k,$$

$$q_{1,2} = B/T \pm \sqrt{(B/T)^2 - 1},$$

where C, D are the arbitrary constants, $q_{1,2}$ are the solutions of the characteristic equation of the homogeneous equation (27).

Then

$$M_k = M_m \frac{q_2^k - q_1^k}{q_2^m - q_1^m}, \quad 0 \le k \le m-1,$$

$$M_k = M_{m+1} \frac{q_2^n q_1^k - q_1^n q_2^k}{q_1^{m+1} q_2^n - q_2^{m+1} q_1^n}, \quad m+2 \le k \le n. \tag{28}$$

After the substitution of the found values by $k = m$ and $k = m+1$, one obtain the system of the two linear algebraic equations relatively to M_m and M_{m+1}.

$$\begin{cases} TM_{m+1} - 2BM_m + TM_m \dfrac{q_2^{m-1} - q_1^{m-1}}{q_2^m - q_1^m} = f\dfrac{\partial}{\partial x} g_\lambda(0, \xi - a_m) \\ TM_{m+1} \dfrac{q_1^{m+2} q_2^n - q_2^{m+2} q_1^n}{q_1^{m+1} q_2^n - q_2^{m+1} q_1^n} - 2BM_{m+1} + TM_m = f\dfrac{\partial}{\partial x} g_\lambda(l, \xi - a_m) \end{cases}.$$

After searching of M_m and M_{m+1} as the solutions of the pointed by the formulas (28) system, one can define M_k, $k = \overline{0, n}$. One can obtain from the moments' equality condition and consider as in tin the three moments' theorem, each of the span separately:

$$(\xi - a_m) f - M_m + M_{m+1} - lV_{\lambda_m}(a_m + 0) = 0,$$

$$-(a_{m+1} - \xi) f - M_m + M_{m+1} - lV_{\lambda_{m+1}}(a_{m+1} - 0) = 0,$$

$$-M_k + M_{k+1} - lV_{\lambda_k}(a_k + 0) = 0, \quad k = \overline{0, n-1}, \quad k \neq m,$$

$$-M_k + M_{k+1} - lV_{\lambda_{k+1}}(a_{k+1} - 0) = 0, \quad k = \overline{0, n-1}, \quad k \neq m.$$

Then taking into consideration (4)

$$N_\lambda(a_k) = (-M_{k-1} + 2M_k - M_{k+1})/l, \quad k \neq m, \quad k \neq m+1;$$

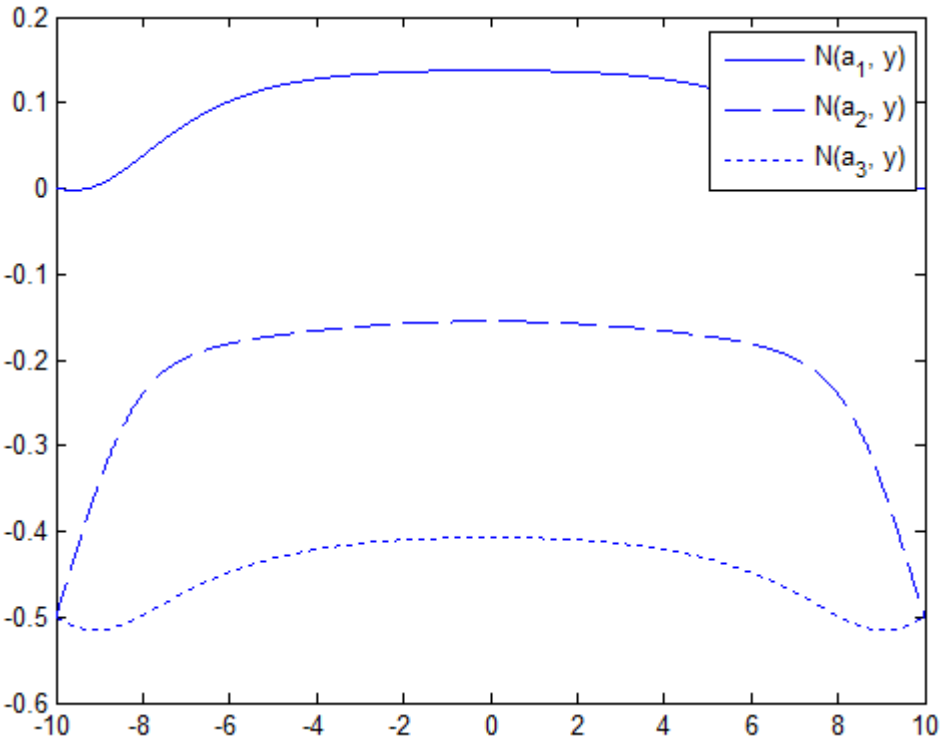
$$N_\lambda(a_m) = (-M_{m-1} + 2M_m - M_{m+1} - (a_{m+1} - \xi)f)/l;$$

$$N_\lambda(a_{m+1}) = (-M_m + 2M_{m+1} - M_{m+2} - (\xi - a_m)f)/l,$$

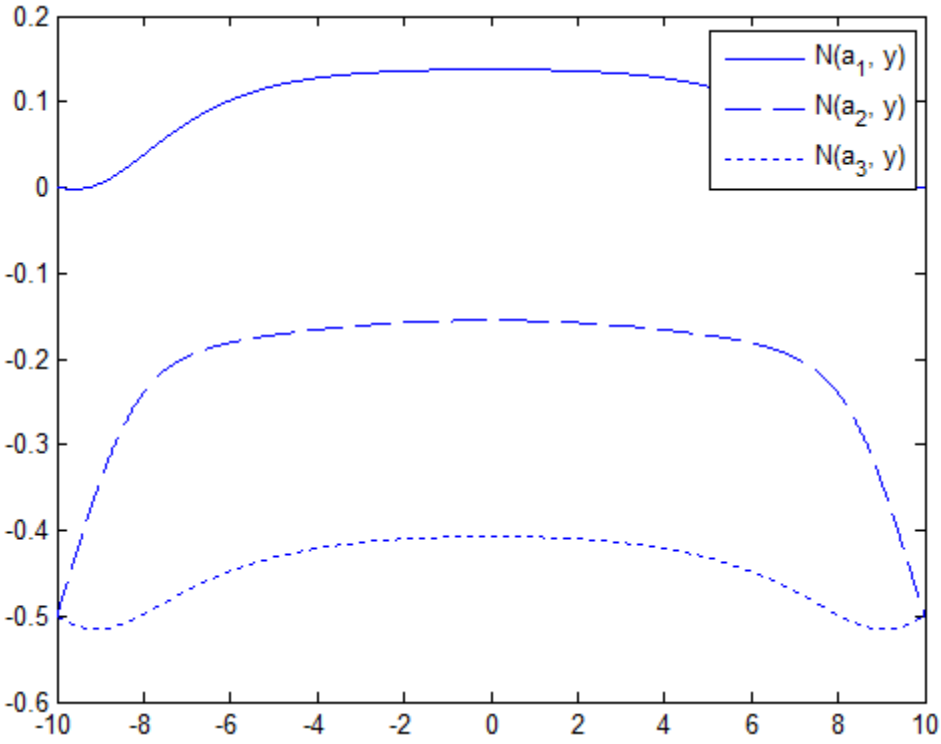
with the help of the inverse Fourier transformation (7) one can find $M_x(a_k, y)$, $N(a_k, y)$, $k = \overline{0, n}$.

The calculations

The graphics of the bending moments $M_x(a_k, y)$ and reactions of the bearings $N(a_k, y)$ are shown for the case $l_1 = 10$, $l_2 = 10$, $l = 4$, $n = 5$, $m = 3$, $\xi = 0$, $\eta = 0$ (Fig. 1). At that the solid line corresponds to the case $k = 1$, the dashdotted line to $k = 2$ and dotted line $k = 3$. The cases $k = 4, 5, 6$ by act of the symmetry are analogical to $k = 3, 2, 1$ correspondently.



a



b

Fig. 1. The graphics of the bending moments $M_x(a_k, y)$ and reactions of the bearings $N(a_k, y)$:

a – $\min\limits_{y\in(-l_1,l_2)} M_x(a_1, y) = -0.0728$, $\min\limits_{y\in(-l_1,l_2)} M_x(a_2, y) = -0.5507$, $\min\limits_{y\in(-l_1,l_2)} M_x(a_3, y) = -1.4526$;

b – $\max\limits_{y\in(-l_1,l_2)} N(a_1, y) = 0.1377$, $\max\limits_{y\in(-l_1,l_2)} N(a_2, y) = -0.1550$, $\max\limits_{y\in(-l_1,l_2)} N(a_3, y) = -0.4071$

Thus, the values of reactions and the bending moments on the bearers were obtained. The proposed approach to resolving such problems provides a solution for continuous plate with curved defects.

References

1. Попов Г.Я. Расчёт коробчатых оболочек / Г.Я. Попов, В.В. Реут // Труды XIV Всесоюзной конференции по пластинкам и оболочкам. – Тбилиси: Изд. Тбилисского ун-та, 1987. – Т. 2. – С. 327–332.
2. Гришин В.А. Напряженное состояние коробчатой оболочки, подкрепленной парой симметричных включений, параллельных ребру оболочки / В.А. Гришин, В.В. Реут. // Прикладная математика и механика. – 1995. – Том 59, Вып. 5. – С. 849-852.
3. Тимошенко С.П. Пластинки и оболочки [Текст] : научное издание : пер. с англ. / С.П. Тимошенко, С. Войновский-Кригер ; пер. В.И. Контовт ; ред. пер. Г.С. Шапиро. – 2-е изд., стер. – М. : Наука, 1966. – 636 с. : ил.
4. Власов В.З. Избранные труды [Текст] / В.З. Власов; Акад. наук СССР. – М. : Изд-во Акад. Наук СССР, 1962. – .
   Т. 1 : «Очерк научной деятельности. Общая теория оболочек» : статьи. – М. : Изд-во Акад. Наук СССР, 1962. – 528 с. : ил.
5. Доннелл Л.Г. Балки, пластины и оболочки [Текст] : научное издание / Л.Г. Доннелл ; пер. Л.Г. Корнейчук ; ред. Э.И. Григолюк. – М. : Наука, 1982. – 568 с. : ил.
6. Попов Г.Я. Концентрация упругих напряжений возле штампов, разрезов, тонких включений и подкреплений [Текст] / Г.Я. Попов. – М. : Наука, 1982. – 342 с.

7. Ляв А. Математическая теория упругости [Текст] / А. Ляв ; пер.с 4 англ. изд. Б.В. Булгакова и В.Я. Натанзона. – М. ; Л. : ОНТИ, 1935. – 674 с.
8. Навчальний посібник з курсу «Рівняння математичної фізики. Метод інтегральних перетворень» [Текст] / авт.-уклад.: Г.Я. Попов, В.В. Реут, Н.Д. Вайсфельд. – Одеса: Астропринт, 2005. – 184 с.

НАПРУЖЕНИЙ СТАН НЕРОЗРІЗНОЇ ПРЯМОКУТНОЇ ПЛАСТИНКИ

С.Т. Роговський, В.В. Реут

Одеський національний університет імені І.І. Мечникова,
вул. Дворянська, 2, Одеса, 65082, Україна: e-mail: reut@onu.edu.ua

Задачі о нерозрізних пластинках з проміжними опорами часто виникають при розрахунках в будівельних конструкціях та елементів конструкцій в машинобудуванні. Як показано в роботах [1, 2], до таких задач зводиться і розрахунок пластинчастих оболонок і складчастих конструкцій. Розрахунку напруженого стану пластин присвячені роботи багатьох вітчизняних і зарубіжних вчених, огляд яких можна знайти в [3, 4, 5]. У даній роботі за допомогою методу інтегральних перетворень [6] і методу трьох моментів [7] побудована функція впливу, що дозволяє розглядати більш складні задачі про напружений стан пластинчастих конструкцій. Наведено розрахунки характерних величин – реакцій і величин згинальних моментів на опорах.

Ключові слова: оболонка, деформація, напружений стан, згинальний момент

НАПРЯЖЕННОЕ СОСТОЯНИЕ НЕРАЗРЕЗНОЙ ПРЯМОУГОЛЬНОЙ ПЛАСТИНКИ

С.Т. Роговский, В.В. Реут

Одесский национальный университет имени И.И. Мечникова,
ул. Дворянская, 2, Одесса, 65082, Украина; e-mail: reut@onu.edu.ua

Задачи о неразрезных пластинках с промежуточными опорами часто возникают при расчетах в строительных конструкциях и элементов конструкций в машиностроении. Как показано в работах [1, 2], к таким задачам сводится и расчет пластинчатых оболочек и складчатых конструкций. Расчету напряженного состояния пластин посвящены работы многих отечественных и зарубежных ученых, обзор которых можно найти в [3, 4, 5]. В настоящей работе с помощью метода интегральных преобразований [6] и метода трёх моментов [7] построена функция влияния, что позволяет рассматривать более сложные задачи о напряжённом состоянии пластинчатых конструкций. Приведены расчёты характерных величин – реакций и величин изгибающих моментов на опорах.

Ключевые слова: оболочка, деформация, напряженное состояние, изгибающий момент

УДК 621.362.2

Informatics and Mathematical Methods in Simulation
Vol. 2 (2012), No. 2, pp. 143-152

ЕЛЕКТРИЧНІ ПАРАМЕТРИ МОДУЛЬНИХ ПЕРЕТВОРЮВАЧІВ ПОСТІЙНОЇ НАПРУГИ З ГРАНИЧНО-РОЗРИВНИМ РЕЖИМОМ ФУНКЦІОНУВАННЯ ПРИ НЕІДЕНТИЧНОСТІ ІНДУКТИВНОСТЕЙ СИЛОВИХ КАНАЛІВ

Ю.О. Гунченко

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: 7996445@mail.ru

В роботі розглянуто особливості електричних процесів у імпульсних перетворювачах постійної напруги модульних структур з гранично-розривним режимом функціонування при неідентичності індуктивностей силових каналів. Отримано й наведено основні розрахункові співвідношення струмів у елементах каналів при різних системах управління, розроблена методика та наведено приклади визначення електричних параметрів елементів силових каналів.

Ключові слова: перетворювач постійної напруги, гранично-розривний режим, силовий канал, модульна структура, електричні параметри

Постановка проблеми

Побудова джерел електроживлення для різноманітного устаткування, які володіють заданими техніко-економічними показниками, забезпечують якісне та надійне живлення, з можливістю масштабування є важливою науково-технічною задачею. Один з важливих показників – надійність системи, до якої входить джерело електроживлення – частіше перетворювач постійної напруги (ППН), принципово не може бути вищою за надійність перетворювача.

Аналіз досліджень і публікацій

Модульні перетворювачі постійної напруги находять широке застосування в джерелах живлення різноманітного призначення, зокрема в джерелах електроживлення відповідального обладнання.

Кількість силових каналів (СК) N (рис. 1) обирається із умов надійності, якості, масагабаритних, динамічних показників, коефіцієнта корисної дії [1, 2]. Додатково зменшити динамічні втрати за рахунок переключення силових ключів – включенні транзисторного і вимкнення діодного ключів при нульовому струмі, поліпшити динамічні показники можливо при граничному чи розривному режимі струму дроселя [2-4].

У відомих роботах [2, 4] отримано математичні моделі і описано електричні процеси як в одному силовому каналі, так і в модульному перетворювачі в цілому при ідентичних параметрах елементів і рівних напругах джерел живлення для СК, що понижують, підвищують та інвертують (рис. 2).

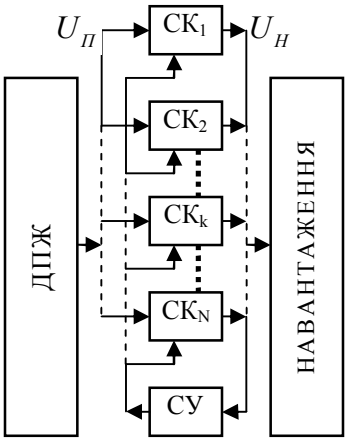


Рис. 1. Структура модульного ППН: ДПЖ – джерело первинного електроживлення, $СК_1$, $СК_2$,…, $СК_k$,…, $СК_N$ – відповідно 1-ий, 2-ий,…, *k*-ий,…, *N*-ий силові канали, СУ – система управління, $U_П$ – напруга живлення СК, $U_Н$ – напруга навантаження СК

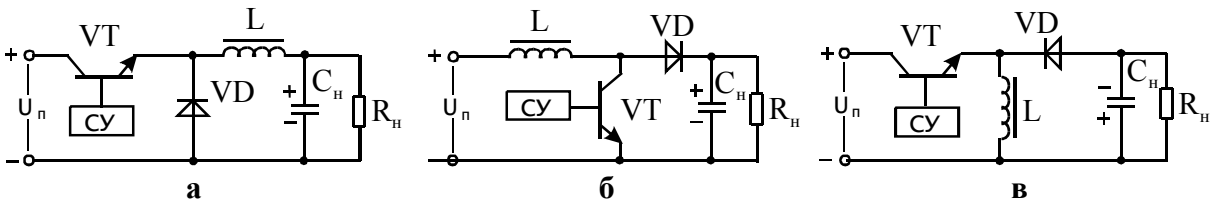


Рис. 2. Схеми силових каналів: а) понижуючої, б) підвищуючої, в) інвертуючої структур

Виділення невирішених раніше частин загальної проблеми

На практиці неможливо отримати повну ідентичність елементів – в першу чергу, дроселів індуктивностей СК, неідентичність яких, в залежності від технології виготовлення, температури, струму, нерівномірного старіння матеріалів, може складати до 30% [5]. Неврахування цього фактора – розкиду параметрів елементів СК, призводить до нерівномірного розподілу навантаження між ними та перевищення допустимих параметрів елементів, які до них входять.

Формулювання цілей статті

Ціллю статті є аналіз електричних параметрів і процесів модульних перетворювачів постійної напруги з гранично-розривним режимом функціонування при неідентичності дроселів L_k силових каналів та створення методики їх розрахунку.

Виклад основного матеріалу дослідження

Регулювання струму дроселя $i_{L_k}(t)$, шляхом зміни тривалості регулюючих імпульсів ($t_{н_k} = \text{var}$) и частоти перетворення ($f_k = 1/T_k = \text{var}$), дозволяє регулювати

напругу навантаження $U_н$ при гарантованому граничному чи розривному режимах у всьому діапазоні регулювання.

В принципі, можлива різна реалізація систем управління (СУ) [1, 6], внаслідок чого електричні процеси в СК будуть також різні. Багатообразність систем управління модульних ППН з граничним і розривним режимом функціонування можливо звести к трьом основним типам (по електричним процесам в силових каналах):

1) СУ з розподіленням одного імпульсу управління на всі СК, при необхідності з відповідним зсувом ($СУ_1$). При цьому виконується умова рівності часу накопичення у всіх СК: $t_{н_k} = t_{н_1}$;

2) СУ з незалежним формуванням імпульсів управління в кожному СК і з негативним зворотним зв'язком по струму навантаження в каналах ($СУ_2$). При цьому виконується умова рівності середніх струмів навантаження СК: $I_{н_{срk}} = I_{н_{ср1}}$;

3) СУ з струмковим регулюванням в ($СУ_3$). При цьому виконується умова рівності амплітудних значень струмів в елементах СК: $I_{m_k} = I_{m_1}$.

Визначимо відношення амплітудних (індекс m), середніх (індекс $ср$), діючих (без індексу) значень струмів в елементах любих двох СК – дроселях I_{mk}, I_{Lcpk}, I_{Lk}, транзисторах I_{mk}, I_{VTcpk}, I_{VTk}, діодах I_{mk}, I_{VDcpk}, I_{VDk}. Для зручності аналізу й запису будемо порівнювати струми любого *k*-ого СК с *1*-им СК, в якому гарантовано досягається граничний режим функціонування. Додаткове допущення – всі СК функціонують з однаковою частотою перетворення, для чого може бути застосована система управління, описана у [6], яка забезпечує функціонування одного СК у граничному режимі, інших у розривному з однаковою частотою перетворення та рівномірним зсувом електричних процесів.

При $СУ_1$ виконується умова:

$$t_{н_k} = t_{н_1}, \tag{1}$$

де $t_{н_1}$, $t_{н_k}$ – відповідно час накопичення енергії в *1*-ом и *k*-ом каналах.

При рівності напруг живлення $U_{п_1} = U_{п_k}$ й навантаження $U_{н_1} = U_{н_k}$ з врахуванням гранично-розривного режиму амплітуду струмів I_{m_k} для любого *k*-ого каналу будь-якої структури (понижуючої, підвищуючої, інвертуючої) можливо записати на інтервалах відповідно накопичення і звороту:

$$I_{m_k} = \frac{1}{L_k}\int_0^{t_{н_k}} u_{L_{н_k}}(t)dt = -\frac{1}{L_k}\int_0^{t_{в_k}} u_{L_{в_k}}(t)dt = \frac{1}{L_k}U_{L_{н_k}}K_{н_k}T_k = -\frac{1}{L_k}U_{L_{в_k}}K_{в_k}T_k, \tag{2}$$

де

$U_{L_{н_k}}$, $U_{L_{в_k}}$ – напруга, що прикладається до дроселю *k*-ого СК відповідно на інтервалах накопичення $t_{н_k}$ і звороту $t_{в_k}$;

L_k – індуктивність дроселя *k*-ого каналу;

T_k – період перетворення;

$K_{н_k} = t_{н_k}/T_k$, $K_{в_k} = t_{в_k}/T_k$ – коефіцієнти накопичення і звороту *k*-ого каналу.

З (2) при рівності $U_{п_1} = U_{п_k}$, $U_{н_1} = U_{н_k}$ також слідує виконання для $СУ_1$ умови:

$$t_{в_k} = t_{в_1}, \quad K_{н_k} = K_{н_1}, \quad K_{в_k} = K_{в_1}. \tag{3}$$

Враховуючі (1) амплітудні значення струмів будь якого *k*-ого каналу виразимо через відповідне амплітудне значення струму першого каналу:

$$I_{m_k} = I_{m_1} L_1 / L_k \ . \tag{4}$$

Оскільки середні і діючі струми прямо пропорційні амплітудному значенню [2, 4], а коефіцієнти накопичення $K_{н_k} = K_{н_1}$ і звороту $K_{в_k} = K_{в_1}$ рівні (3), при СУ$_1$, середні і діючі струми елементів схем СК розподіляються аналогічно амплітудним значенням струмів, зворотно пропорційно індуктивностям дроселів каналів, при цьому всі СК функціонують в граничному режимі:

$$\begin{cases} I_{Lcp_k} = \dfrac{1}{2} I_{m_k} \left(K_{н_k} + K_{в_k} \right) = I_{Lcp_1} L_1 / L_k \\ I_{VT\,cp_k} = \dfrac{1}{2} I_{m_k} K_{н_k} = I_{VT\,cp_1} L_1 / L_k \\ I_{VD\,cp_k} = \dfrac{1}{2} I_{m_k} K_{в_k} = I_{VD\,cp_1} L_1 / L_k \\ I_{L_k} = \dfrac{I_{m_k}}{\sqrt{3}} \left(\sqrt{K_{н_k}} + \sqrt{K_{в_k}} \right) = I_{L_1} L_1 / L_k \\ I_{VT_k} = I_{m_k} \sqrt{K_{н_k} / 3} = I_{VT_1} L_1 / L_k \\ I_{VD_k} = I_{m_k} \sqrt{K_{в_k} / 3} = I_{VD_1} L_1 / L_k \end{cases} . \tag{5}$$

За перший «базовий» можна прийняти будь який СК та застосувати для нього формули граничного режиму [2, 4], так як всі канали при СУ$_1$ функціонують в граничному режимі (рис. 3(а)).

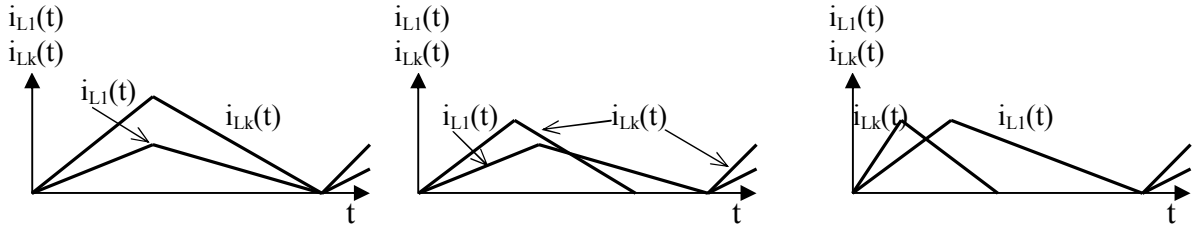


Рис. 3. Діаграми струмів дроселів *1*-ого и *k*-ого СК при $L_k = \dfrac{1}{2} L_1$: а) СУ$_1$, де $I_{m_k} = 2 I_{m_l}$, $t_{н_k} = t_{н_1}$, $t_{в_k} = t_{в_1}$; б) СУ$_2$, де $I_{m_k} = \sqrt{2} I_{m_l}$, $t_{н_k} = \sqrt{\dfrac{1}{2}} t_{н_1}$, $t_{в_k} = \sqrt{\dfrac{1}{2}} t_{в_1}$; в) СУ$_3$, де $I_{m_k} = I_{m_l}$, $t_{н_k} = \dfrac{1}{2} t_{н_1}$, $t_{в_k} = \dfrac{1}{2} t_{в_1}$

При СУ$_2$ виконується умова рівності середніх струмів навантаження СК:

$$I_{н_{ср k}} = I_{н_{ср 1}} \ . \tag{6}$$

Розглянемо розподіл струмів в СК на прикладі понижуючої структури, для якої струм навантаження відповідає струму дроселя $I_{н_{срk}} = I_{L_{срk}}$ [2].

Середній струм дроселя *k*-ого силового каналу дорівнює середньому струму дроселя першого каналу:

$$I_{L_{срk}} = \frac{1}{2} I_{m_k} \left(K_{н_k} + K_{в_k} \right) = I_{L_{ср1}} = \frac{1}{2} I_{m_1} \left(K_{н_1} + K_{в_1} \right). \quad (7)$$

При підстановці в (6) значень коефіцієнтів накопичення і звороту з (2) отримаємо:

$$\frac{1}{2} I_{m_k} \left(\frac{I_{m_k} L_k}{U_{Lн} T} - \frac{I_{m_k} L_k}{U_{Lв} T} \right) = \frac{1}{2} I_{m_1} \left(\frac{I_{m_1} L_1}{U_{Lн} T} - \frac{I_{m_1} L_1}{U_{Lв} T} \right) \Rightarrow I_{m_k} = I_{m_1} \sqrt{L_1 / L_k} \, . \quad (8)$$

При цьому амплітудні значення струмів в елементах СК розподіляються зворотно пропорційно кореням квадратним індуктивностей дроселів каналів. Аналогічний результат отримано для структур, що підвищують і інвертують .

Підставляючи (8) в (2), визначимо розподіл коефіцієнтів накопичення та звороту в СК:

$$K_{н_k} = K_{н_1} \sqrt{L_k / L_1} \, , \quad K_{в_k} = K_{в_1} \sqrt{L_k / L_1} \, . \quad (9)$$

Діючі струми в елементах СК при підстановці (8) і (9) в (5) розподіляться наступним чином:

$$\begin{cases} I_{L_k} = I_{L_1} \left(L_1 / L_k \right)^{1/4} \\ I_{VT_k} = I_{VT_1} \left(L_1 / L_k \right)^{1/4} \\ I_{VD_k} = I_{VD_1} \left(L_1 / L_k \right)^{1/4} \end{cases} . \quad (10)$$

При цьому СК з максимальним значенням індуктивності буде функціонувати в граничному режимі, інші – в розривному режимі (рис. 3(б)). Відповідно за базовий «перший» слід прийняти СК с $L_1 = L_{\max}$, для якого підійдуть співвідношення граничного режиму [2, 4].

При СУ$_3$ виконується умова рівності амплітудних значень струмів в каналах:

$$I_{m_k} = I_{m_1} \, . \quad (11)$$

Підставляючи (11) в (2), визначимо розподіл коефіцієнтів накопичення і звороту в СК:

$$K_{н_k} = K_{н_1} L_k / L_1 \, , \quad K_{в_k} = K_{в_1} L_k / L_1 \, . \quad (12)$$

Коефіцієнти накопичення і звороту в каналах розподіляються прямо пропорційно індуктивностям каналів.

Середні і діючі струми в елементах каналів отримаємо, підставляючи (11) та (12) в (5):

$$\begin{cases} I_{L_{cpk}} = I_{L_{cp1}} L_k / L_1 \\ I_{VT_{cpk}} = I_{VT_{cp1}} L_k / L_1 \\ I_{VD_{cpk}} = I_{VD_{cp1}} L_k / L_1 \\ I_{L_k} = I_{L_1} \sqrt{L_k / L_1} \\ I_{VT_k} = I_{VT_1} \sqrt{L_k / L_1} \\ I_{VD_k} = I_{VD_1} \sqrt{L_k / L_1} \end{cases}. \qquad (13)$$

Середні струми в СК розподіляються прямо пропорційно, а діючі струми прямо пропорційно квадратним кореням значень індуктивностей каналів.

При $СУ_3$, аналогічно $СУ_2$, силовий канал з максимальною індуктивністю функціонує в граничному режимі (рис. 3(в)), відповідно його слід прийняти за базовий «перший».

На рис. 4 приведено залежності відношень амплітудних значень струмів елементів I_{m_k} / I_{m_1} (рис. 4(а)), середніх значень $I_{L_{cpk}} / I_{L_{cp1}}$, $I_{VT_{cpk}} / I_{VT_{cp1}}$, $I_{VD_{cpk}} / I_{VD_{cp1}}$ (рис. 4(б)) та діючих значень струмів в елементах СК I_{L_k} / I_{L_1}, I_{VT_k} / I_{VT_1}, I_{VD_k} / I_{VD_1} (рис. 4(в)) від відношення індуктивностей СК.

Аналіз отриманих співвідношень і залежностей показує:

1) Електричні процеси при неідентичності дроселів в СК залежать від типу системи управління і не залежить від типу силового каналу.

2) При $СУ_1$ всі силові канали можуть функціонувати у граничному режимі. При $СУ_2$ та $СУ_3$ – в граничному режимі функціонує СК з максимальним значенням індуктивності, інші – в розривному.

3) Неідентичність дроселів в більший степені впливає (рис. 3) на струми елементів силових каналів з $СУ_1$, відповідно елементи СК з $СУ_1$ необхідно обирати з більшим запасом по струму і потужності, що розсіюється.

4) Найбільш близькі по значенням діючих струмів і, відповідно, по потужності, що розсіюється і температурним режимам однотипні елементи СК з $СУ_2$.

Виходячи з вищевикладеного, пропонується методика визначення електричних параметрів для любого *k*-ого СК модульної структури, яка складається із 5 основних шагів.

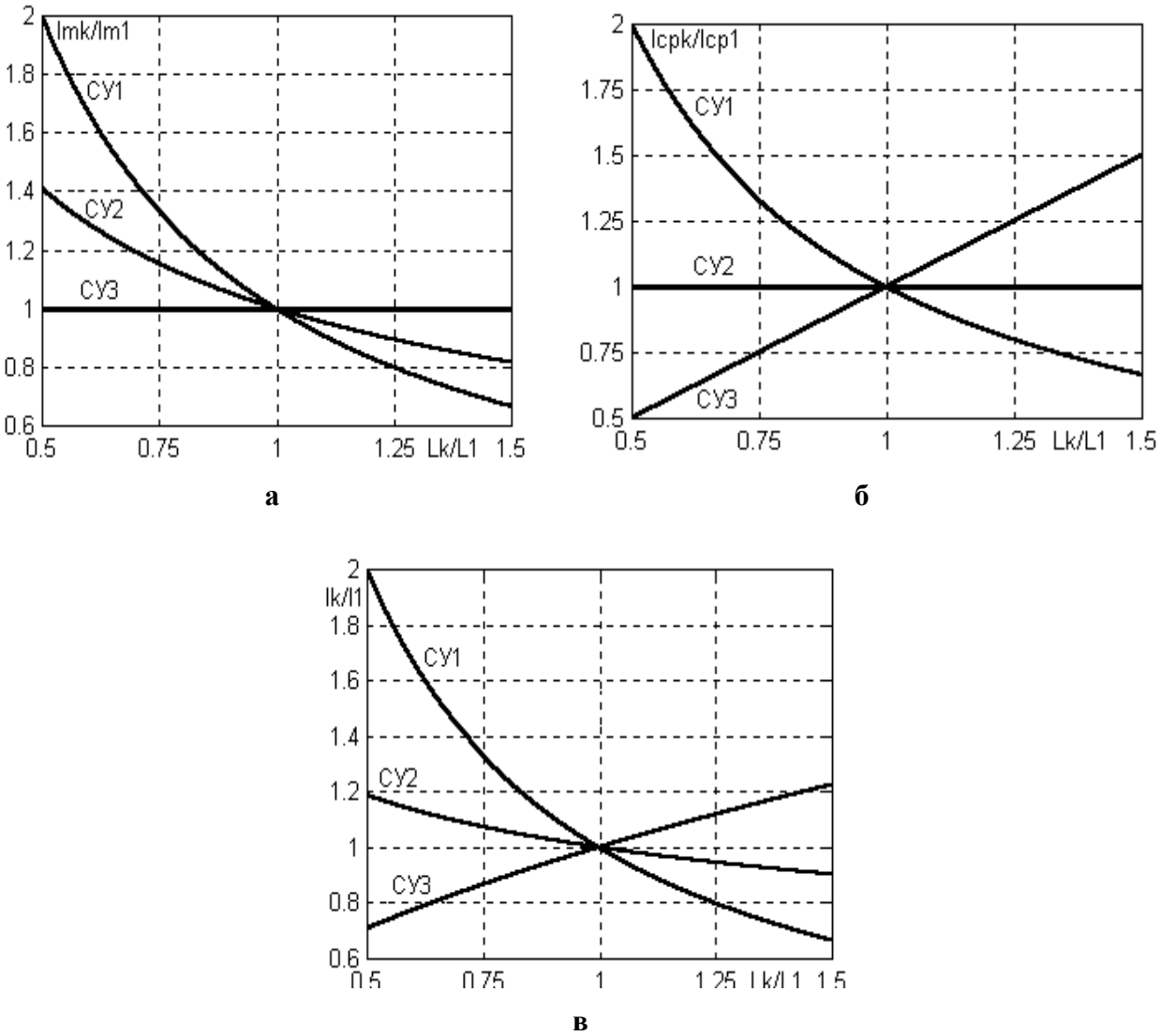
Шаг 1. Вибір першого «базового» каналу. Визначаємо СК (вважаємо його першим), гарантовано функціонуючого в граничному режимі. Цім каналом буде СК с максимальним значенням індуктивності $L_1 = L_{\max}$ для $СУ_2$ и $СУ_3$ і будь який СК для $СУ_1$ при неідентичності дроселів.

Шаг 2. Визначення параметрів граничного режиму. Для першого СК, що функціонує в граничному режимі, визначаємо [4] коефіцієнти накопичення $K_{н_1}$, звороту $K_{в_1}$.

Шаг 3. Із умови рівності суми середніх струмів по колам навантаження СК струму навантаження $\sum_{k=1}^{N} I_{н_{cpk}} = I_{н_{cp}} = \frac{U_н}{R_н}$, умови відповідності струму навантаження струму дроселя $i_{н_k}(t) = i_{L_k}(t)$ (для структури, що понижує) чи струму діода $i_{н_k}(t) = i_{VD_k}(t)$ (для структур, що підвищує та інвертує) і їх співвідношень (5) для $СУ_1$, (6) для $СУ_2$, (13) для $СУ_3$ при не ідентичності дроселів визначаємо середній струм дроселя $I_{L_{cp1}}$ (для структури, що понижує) чи діода $I_{VD_{cp1}}$ (для структури, що підвищує чи інвертує) першого СК.

Шаг 4. Визначення амплітудних, середніх, діючих значень струмів елементів першого СК і частоти перетворення. Із середнього струму дроселя чи діода (шаг 3) и параметрів граничного режиму (шаг 2) визначаємо (5) амплітудні значення струму I_{m1}, середні и діючи значення струмів елементів першого СК а також [4] частоту перетворення f_1, при цьому найдена частота загальна для всіх СК.

Шаг 5. Визначення струмів та параметрів *k*-ого СК. По співвідношенням (3-5) для $СУ_1$, (6, 8-10) для $СУ_2$, (11-13) для $СУ_3$ при не ідентичності дроселів визначаємо електричні параметри (струми в елементах, коефіцієнти накопичення і звороту) для любого *k*-ого СК.



а **б** **в**

Рис. 4. Залежності відношень а) амплітудних, б) середніх, в) діючих значень струмів в СК з системами управління $СУ_1$, $СУ_2$, $СУ_3$

Приклад 1. Структура, що понижує з $СУ_1$ і неідентичністю дроселів СК.

Шаг 1. Обираємо перший СК L_1 (будь який).

Шаг 2. Визначаємо із [4] параметри граничного режиму (1-ого СК):

$$K_{н_1} = U_н / U_п , \quad K_{в_1} = 1 - K_{н_k} .$$

Шаг 3. Так як в структурі, що понижує, струмом навантаження є струм дроселя, з урахуванням (5) запишемо систему рівнянь, звідки визначимо величину середнього струму дроселя першого СК:

$$\begin{cases} I_{L_{cp2}} = I_{Lcp_1} L_1/L_2 \\ I_{L_{cp3}} = I_{Lcp_1} L_1/L_3 \\ \vdots \\ I_{L_{cpN}} = I_{Lcp_1} L_1/L_N \Rightarrow I_{Lcp_1} = \dfrac{U_н/R_н}{1+L_1\sum\limits_{k=2}^{N}\dfrac{1}{L_k}}. \\ \sum\limits_{k=1}^{N} I_{Lcp_k} = \dfrac{U_н}{R_н} \end{cases}$$

Шаг 4. Визначаємо струми (5) елементів першого СК и частоту функціонування [4].

$$I_{m_1} = 2I_{L_{cp1}}, \quad I_{VT_{cp1}} = I_{m_1}K_{н_1}/2, \quad I_{VD_{cp1}} = I_{m_1}K_{в_1}/2, \quad f_1 = \frac{U_н K_{в_1}}{L_1 I_{m_1}},$$

$$I_{L_1} = I_{m_1}\left(\sqrt{K_{н_1}} + \sqrt{K_{в_1}}\right)\Big/\sqrt{3}, \quad I_{VT_1} = I_{m_1}\sqrt{K_{н_1}/3}, \quad I_{VD_1} = I_{m_1}\sqrt{K_{в_1}/3}.$$

Шаг 5. Визначаємо струми елементів і параметри (3-5) *k*-их СК.

$$K_{н_k} = K_{н_1}, \quad K_{в_k} = K_{в_1}, \quad I_{m_k} = I_{m_1}L_1/L_k, \quad I_{L_{cpk}} = I_{L_{cp1}}L_1/L_k,$$

$$I_{VT_{cpk}} = I_{VT_{cp1}}L_1/L_k, \quad I_{VD_{cpk}} = I_{VD_{cp1}}L_1/L_k, \quad I_{L_k} = I_{L_1}L_1/L_k,$$

$$I_{VT_k} = I_{VT_1}L_1/L_k, \quad I_{VD_k} = I_{VD_1}L_1/L_k.$$

Таким чином, визначено всі основні електричні параметри модульного ППН понижуючого типу с СУ$_1$.

Приклад 2. Структура, що підвищує з СУ$_3$.

Шаг 1. Обираємо перший СК $L_1 = L_{\max}$.

Шаг 2. Визначаємо із [4] параметри граничного режиму (1-ого СК):

$$K_{н_1} = \frac{U_н - U_п}{U_н}, \quad K_{в_1} = 1 - K_{н_k} = \frac{U_п}{U_н}.$$

Шаг 3. Так як для структури, що підвищує, струм навантаження відповідає струму діода, з урахуванням (13) запишемо систему рівнянь, звідки визначимо величину середнього струму діода першого СК:

$$\begin{cases} I_{VD_{cp2}} = I_{VDcp_1} L_2/L_1 \\ I_{VD_{cp3}} = I_{VDcp_1} L_3/L_1 \\ \vdots \\ I_{VD_{cpN}} = I_{VDcp_1} L_N/L_1 \Rightarrow I_{VDcp_1} = \dfrac{U_н/R_н}{1+1\Big/L_1\sum\limits_{k=2}^{N}L_k}. \\ \sum\limits_{k=1}^{N} I_{VDcp_k} = \dfrac{U_н}{R_н} \end{cases}$$

Шаг 4. Визначаємо струми (5) елементів першого СК и частоту функціонування [4].

$$I_{m_1} = 2I_{VD_{cp_1}} / K_{в_1}, \quad I_{L_{cp_1}} = I_{m_1}/2, \quad I_{VT_{cp_1}} = I_{m_1} K_{н_1}/2, \quad f_1 = \frac{U_н K_{н_1} K_{в_1}}{L_1 I_{m_1}},$$

$$I_{L_1} = I_{m_1}\left(\sqrt{K_{н_1}} + \sqrt{K_{в_1}}\right)/\sqrt{3}, \quad I_{VT_1} = I_{m_1}\sqrt{K_{н_1}/3}, \quad I_{VD_1} = I_{m_1}\sqrt{K_{в_1}/3}.$$

Шаг 5. Визначаємо струми елементів и параметри (11-13) *k*-их СК.

$$K_{н_k} = K_{н_1} L_k / L_1, \quad K_{в_k} = K_{в_1} L_k / L_1, \quad I_{m_k} = I_{m_1}, \quad I_{L_{cpk}} = I_{L_{cp1}} L_k / L_1,$$

$$I_{VT_{cpk}} = I_{VT_{cp1}} L_k / L_1, \quad I_{VD_{cpk}} = I_{VD_{cp1}} L_k / L_1, \quad I_{L_k} = I_{L_1}\sqrt{L_k / L_1},$$

$$I_{VT_k} = I_{VT_1}\sqrt{L_k / L_1}, \quad I_{VD_k} = I_{VD_1}\sqrt{L_k / L_1}.$$

Таким чином, визначено всі основні струми і параметри модульного ППН підвищуючого типу з $СУ_3$.

Висновки і перспективи подальших досліджень першого

1) Класифіковано системи управління модульними ППН з гранично-розривним функціонуванням.

2) Розроблено математичні моделі співвідношень амплітудних, середніх, діючих струмів в елементах СК, включених модульно при неідентичності індуктивностей дроселів силових каналів для основних структур и систем управління.

3) Розроблена методика визначення електричних параметрів – струмів в елементах СК, коефіцієнтів накопичення і звороту, частоти перетворення при неідентичності індуктивностей дроселів і напруг живлення каналів, узагальнена для основних структур силових каналів и систем управління, що дозволяє отримані математичні моделі використовувати для наукових та інженерних розрахунків, що проілюстровано прикладами.

В перспективах подальших досліджень можна виділити розробку математичних моделей для випадків неідентичності напруг електроживлення, дослідження електричних процесів, розробку методик проектування модульних джерел живлення при найбільш можливих розкидуваннях параметрів елементів й з застосування ймовірних методів визначення режимів по заданим допускам та законам розподілу параметрів елементів.

Список літератури

1. Мелешин В.И. Транзисторная преобразовательная техника [Текст] / В.И. Мелешин. – М. : Техносфера, 2005. – 627 с.: рис., табл.
2. Кадацкий А.Ф. Электрические процессы в модульных импульсных преобразователях постоянного напряжения с граничным режимом функционирования / А.Ф. Кадацкий, Ю.А. Гунченко // Наукові праці ОНАЗ ім. О.С. Попова. – 2004. – №1. – С. 9-15.
3. Гунченко Ю.А. Использование частотно-широтно-импульсной модуляции в преобразователях напряжения / Ю.А. Гунченко // Материалы 7-го международного молодежного форума «Радиоэлектроника и молодежь в XXI веке». – Харьков: ХНУРЭ, 2003. – С. 189.

4. Кадацкий А.Ф. Электрические процессы в импульсных преобразователях постоянного напряжения с граничным режимом функционирования / А.Ф. Кадацкий, Ю.А. Гунченко // Праці УНДІРТ. – 2003. – №3 (35). – С. 83-85.
5. Ферриты и ферритовые изделия для источников вторичного электропитания. Справочное пособие / В.И. Хандогин, А.В. Райкова, А.В. Куневич и др.: Под ред. В.И. Хандогина. – М: Радио и связь, 1990. – 137 с.
6. Гунченко Ю.А. Управление многофазным импульсным преобразователем постоянного напряжения с гранично-разрывным режимом функционирования / Ю.А. Гунченко // Технология и конструирование в электронной аппаратуре. – 2007. – №6 (72). – С. 20-25.

ЭЛЕКТРИЧЕСКИЕ ПРОЦЕССЫ МОДУЛЬНЫХ ПРЕОБРАЗОВАТЕЛЕЙ ПОСТОЯННОГО НАПРЯЖЕНИЯ С ГРАНИЧНО-РАЗРЫВНЫМ РЕЖИМОМ ФУНКЦИОНИРОВАНИЯ ПРИ НЕИДЕНТИЧНОСТИ ИНДУКТИВНОСТЕЙ СИЛОВЫХ КАНАЛОВ

Ю.А. Гунченко

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: 7996445@mail.ru

Рассмотрены особенности электрических процессов в импульсных преобразователях постоянного напряжения (ППН) модульных структур с гранично-разрывным режимом функционирования при неидентичности дросселей силовых каналов (СК). Получены и приведены основные расчетные соотношения токов в элементах каналов при различных системах управления, разработана методика и приведены примеры определения электрических параметров СК.
Ключевые слова: преобразователь постоянного напряжения, гранично-разрывный режим, силовой канал, электрические параметры

ELECTRIC PROCESSES IN MODULAR DC CONVERTERS WITH THE BOUNDARY-DISCONTINUOUS OPERATING MODE BY NONIDENTICAL INDUCTANCES POWER CHANNELS

Yuriy A. Gunchenko

Odessa National Polytechnic University,
1 Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: 7996445@mail.ru

Electric processes in modular DC converters with the boundary-discontinuous operating mode by nonidentical inductances power channels are described. Received and summarizes the estimated ratio of currents in the channels under different control systems. The method of determining electrical parameters of power channels is developed.
Keywords: DC converter, boundary-discontinuous mode, power channel, electric processes

УДК 683.3

Informatics and Mathematical Methods in Simulation
Vol. 2 (2012), No. 2, pp. 153-157

РОЗРОБКА ПЕРЕВІРЯЮЧИХ ТЕСТІВ ДЛЯ ДІАГНОСТУВАННЯ АНАЛОГОВИХ ПРИСТРОЇВ ДИНАМІЧНИМ МЕТОДОМ

П.А. Шкуліпа[1], **М.К. Жердєв**[2], **Г.Б. Жиров**[2]

[1] Одеська державна академія технічного регулювання та якості,
вул. Ковальська, 15, Одеса, 65020, Україна
[2] Військовий інститут Київського національного університету імені Тараса Шевченка,
вул. Ломоносова, 81а, Київ, 03680, України

Розробляється перевіряючий тест для аналогового пристрою, що працює як система автоматичного управління динамічним методом діагностування. Це дозволяє застосувати динамічний метод діагностування до широкого класу аналогових пристроїв.

Ключові слова: динамічний метод, перевіряючий тест, аналоговий пристрій

Вступ

Працездатність аналогового пристрою (АП), що працює як система автоматичного управління в динамічному режимі, найбільш об'єктивно може бути оцінена за допомогою показників якості перехідного процесу (ПП). У процесі функціонування аналоговий пристрій переходить із одного стану в інший. У зв'язку з тим, що вихідним є справний стан і він визначений, найбільш істотним варто вважати визначення оператора переходу системи в ті або інші стани. Перехід АП в різні стани відбувається під впливом виникнення несправностей.

Методи одержання перехідної функції досить широко розглянуті в класичній теорії. Характеристика працездатності системи в загальному випадку може бути отримана в результаті аналізу ПП при різних несправностях, кількісно виражених варіаціями коефіцієнтів системи. Виникає задача визначення тестових впливів на аналоговий пристрій для створення на його виході перехідного процесу.

Основна частина

В роботі розглядаються аналогові пристрої, що працюють як система автоматичного управління в динамічному режимі. Пропонується їх працездатність перевіряти динамічним методом діагностування. Суть динамічного методу діагностування АП, що працюють як система автоматичного управління, полягає в тому, що оцінка їх працездатності проводиться по показниках якості перехідного процесу.

Аналоговий пристрій з декількома входами й виходами можна розглядати як множину елементарних модулів з одним входом і виходом. У цьому випадку кожен елементарний модуль можна представити структурною схемою, на якій його складові елементи зображуються у вигляді з'єднання динамічних ланок. Ця структурна схема описує фізично реалізований аналоговий пристрій із зосередженими параметрами.

Аналоговий пристрій, який представлений структурною схемою, можна описати системою диференціальних рівнянь методом простору станів, що має вигляд [1]:

$$\left.\begin{aligned} \frac{d\vec{X}(t)}{dt} &= \mathbf{A}\vec{X}(t) + \mathbf{B}\vec{U}(t) \\ \vec{Y}(t) &= \mathbf{C}\vec{X}(t) + \mathbf{D}\vec{U}(t) \end{aligned}\right\}, \tag{1}$$

де

$\vec{X}(t) = |x_1(t), x_2(t), ..., x_n(t)|^T$ – n-мірна матриця-стовпець змінних станів;

$\vec{U}(t) = |u_1(t), u_2(t), ..., u_m(t)|^T$ – тестовий вплив;

$\vec{Y}(t) = |y_1(t), y_2(t), ..., y_p(t)|^T$ – реакція на вхідний вплив.

У працездатному стані аналогові пристрої є такими, що управляються й спостерігаються. Елемент є таким, що управляється, якщо для будь-яких моментів часу t_0 і t_1, $t_1 > t_0$, і будь-яких заданих станів x_0 і x_1 існує управляючий сигнал $u(t)$ ($t_0 < t < t_1$), що переводить початковий стан $x(t_0) = x_0$ у будь-який кінцевий $x(t_1) = x_1$. Лінійний n-мірний елемент (1) є таким, що повністю управляється тільки тоді, коли матриця

$$\mathbf{K} = \left|\mathbf{B} \cdot \mathbf{AB} \cdot \mathbf{A^2B} \cdot \ldots \cdot \mathbf{A^{n-1}B}\right|^T \tag{2}$$

має ранг рівний n: $rank(k) = n$ [2].

Елемент $x(t)$ є таким, що спостерігається, якщо в момент спостереження t_0 можна однозначно визначити $x(t_0)$ за даними виміру $y(t)$ на кінцевому інтервалі часу $t_0 < t < t_1$, $t_1 > t_0$. Для того, щоб елемент, що спостерігається був таким, що повністю управляється й спостерігається, необхідно й достатньо, щоб ранг складеної матриці $\mathbf{K^H}$ виду $\left|\mathbf{C^T} \cdot \mathbf{A^T C^T} \cdot \mathbf{A^{2T} C^T} \cdot \ldots \cdot \left(\mathbf{A^{n-1}}\right)^{\mathbf{T}} \mathbf{C^T}\right|$ дорівнював n [2], тобто,

$$rank\left|\mathbf{K^H}\right| = rank\left|\mathbf{C^T} \cdot \mathbf{A^T C^T} \cdot \mathbf{A^{2T} C^T} \cdot \ldots \cdot \left(\mathbf{A^{n-1}}\right)^{\mathbf{T}} \mathbf{C^T}\right| = n\,. \tag{3}$$

При виконанні умов (2), (3) система рівнянь для елемента приводиться до вигляду

$$\left.\begin{aligned} \frac{d\vec{X}(t)}{dt} &= \mathbf{A}_k\vec{X}(t) + \mathbf{B}_k\vec{U}(t) \\ \vec{Y}(t) &= \mathbf{C}_k\vec{X}(t) \end{aligned}\right\}, \tag{4}$$

де $\mathbf{A}_k$, $\mathbf{B}_k$, $\mathbf{C}_k$ мають вигляд

$$\mathbf{A}_k = \begin{bmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ 0 & 0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ -a_0 & -a_1 & -a_2 & \ldots & -a_{n-1} \end{bmatrix}, \quad \mathbf{B}_k = \begin{bmatrix} 1 \\ 0 \\ 0 \\ \ldots \\ 0 \end{bmatrix}, \tag{5}$$

$$\mathbf{C}_k = \begin{bmatrix} b_0 & b_1 & \ldots & b_m & 0 & \ldots & 0 \end{bmatrix}.$$

Це дозволяє визначити параметри перевіряючого тесту (ПТ) для діагностування аналогового пристрою динамічним методом.

Для побудови ПТ введемо обмеження. Елемент є таким, що управляється і спостерігається з одним входом і виходом. Відоме розташування нулів і полюсів комплексної передаточної функції для елемента на комплексній площині. Оскільки робоча точка АП перебуває на середині лінійної ділянки його вольт-амперної характеристики, то обмежимося тільки двома різнополярними сигналами у вигляді одиничної функції $1(t)$ у якості перевіряючого тесту. Тому спочатку необхідно знайти числові значення їхньої амплітуди ψ_1 і ψ_2.

Для рішення цієї задачі була використана перетворена система рівнянь (4), що зв'язує вхідний і вихідний сигнал в аналоговому пристрої.

Рішення (4) на інтервалі часу $[t_k;t_{k+1}]$ (інтервалі дії одного імпульсу в ПТ має вигляд

$$X(t)|_{[t_k;t_{k+1}]}= e^{A(t_{k+1}-t_k)}X(t_k)+\int_{t_k}^{t_{k+1}} Ce^{A(t_{k+1}-\tau)}BU(\tau)d\tau\,. \qquad (6)$$

Перший доданок у виразі (6) визначається початковими умовами, другий доданок – вхідним впливом. Уведемо позначення $\Phi(t_{k+1}-t_k)=e^{A(t_{k+1}-t_k)}$ й представимо рішення (6) у вигляді

$$X(t)|_{[t_k;t_{k+1}]}= \Phi(t_{k+1}-t_k)X(t_k)+\int_{t_k}^{t_{k+1}} C\Phi(t_{k+1}-\tau)BU(\tau)d\tau\,. \qquad (7)$$

Одержимо загальне рішення для (7) на довільному *k*-ому інтервалі часу. Для цього у вираз (7) замість t_k, t_{k+1} підставляються значення $t_k=k$ і $t_{k+1}=(k+1)T$. Вираз (7) набуває вигляду

$$X(t)|_{[kT;(k+1)T]}= \Phi[(k+1)T-kT]X(kT)+\int_{kT}^{(k+1)T} C\Phi[(k+1)T-\tau]BU(\tau)d\tau\,. \qquad (8)$$

Підставимо у вираз (8) замість узагальненого значення вхідної змінної $U(\tau)$ значення амплітуди імпульсів у перевіряючому тесті. На інтервалах $[t_k=k;t_{k+1}=(k+1)T]$ амплітуда імпульсів у ПТ величина постійна, це дозволяє представити вираз (8) у вигляді

$$X(t)|_{[kT;(k+1)T]}= \Phi[(k+1)T-kT]X(kT)+\int_{kT}^{(k+1)T} C\Phi[(k+1)T-\tau]B\psi_k d\tau\,. \qquad (9)$$

Після взяття визначеного інтеграла у виразі (9) одержимо

$$X(t)|_{[kT;(k+1)T]}= \Phi[(k+1)T-kT]X(kT)+[\Phi(T)-I]A^{-1}B\psi_k\,, \qquad (10)$$

де I – одинична матриця.

Для одержання рішення при реалізації всієї ПТ уведемо позначення $W=[\Phi(T)-I]A^{-1}B$. Оскільки аналітичний вираз не залежить від k і має вигляд, одна-

ковий для всіх інтервалів часу $\left[t_k = k; t_{k+1} = (k+1)T\right]$, вираз (10) представляється у вигляді

$$X(t)|_{[kT;(k+1)T]} = \Phi\left[(k+1)T - kT\right]X(kT) + W\psi_k . \qquad (11)$$

При нульових початкових умовах і одному вхідному впливі у вигляді одиничної функції з амплітудою $\psi_0 = 1(t)$, на інтервалі часу $[0;T]$ вираз (11) приймає вигляд

$$X(t)|_{[0;T]} = \Phi\left[T - 0\right]X(0) + W\psi_0 = W\psi_0 . \qquad (12)$$

Вираз (12) у момент часу $t = T$ з урахуванням початкових умов і прийнятих позначень має вигляд

$$X(t)|_{[0;T]} = W\psi_0 .$$

При вхідному ТВ у вигляді одиничної функції з амплітудою ψ_1 на інтервалі часу $[T;2T]$ вираз (11) має вигляд

$$X(t)|_{[T;2T]} = \Phi\left[T\right]X(T) + W\psi_1 = \Phi\left[T\right]W\psi_0 + W\psi_1 . \qquad (13)$$

Аналогічним способом проводиться послідовна підстановка для всіх інтервалів часу. Після виносу W за дужки реакція на ПТ визначається виразом

$$X\left[(k_0+1)T\right] = \left\{\left[\Phi(T)\right]^n\psi_0 + \left[\Phi(T)\right]^{n-1}\psi_1 + \left[\Phi(T)\right]^{n-2}\psi_2 + \ldots + \psi_n I_n\right\}W . \qquad (14)$$

Оскільки T, ψ_0, k_0 відомі, знайдемо з виразу (14) значення амплітуди одиничної функції в перевіряючому тесті. Для цього перетворимо вираз (14) шляхом нормування по ψ_0 до вигляду

$$\frac{X\left[(k_0+1)T\right]}{\psi_0} = \left\{\left[\Phi(T)\right]^n\psi_0 + \left[\Phi(T)\right]^{n-1}\psi_1 + \left[\Phi(T)\right]^{n-2}\psi_2 + \ldots + \psi_n I_n\right\}\frac{W}{\psi_0} . \qquad (15)$$

Необхідно знайти значення ψ_k, при яких сигнал на виході дорівнює нулю. Прирівняємо вираз (15) до нуля й знайдемо чисельні значення, при яких отримане рівняння має ненульові рішення. Відповідно до методики, викладеної в [3], перша відносна амплітуда розраховується по формулі

$$\frac{\psi_1}{\psi_0} = -\sum_{i=1}^{n} e^{\nu_i T} . \qquad (16)$$

Амплітуда другого імпульсу в тестовому впливі протилежна за знаком і розраховується відповідно до виразу

$$\frac{\psi_2}{\psi_0} = -\sum_{i=1}^{n-1}\sum_{j=i+1}^{n} e^{(\nu_i+\nu_j)T} . \qquad (17)$$

Таким чином, ПТ для аналогового пристрою являє собою послідовність двох різнополярних одиничних функцій з амплітудами ψ_1 (16) і ψ_2 (17).

Висновки

Визначено аналітичні залежності перевіряючих тестів для широкого класу лінійних аналогових пристроїв, що працюють в динамічному режимі. Застосування розроблених перевіряючи тестів для динамічного методу відповідає вимогам діагностування при визначенні поточного рівня працездатності аналогових пристроїв.

Список літератури

1. Зайцев Г.Ф. Теорія автоматичного управління [Текст] : Підручник для студ. вищ. навч. закл. / Г.Ф. Зайцев [и др.] ; ред. Г.Ф. Зайцев. – К. : Техніка, 2002. – 687 с.: рис.
2. Алексеенко А.Г. Микросхемотехника : учеб. пособие для вузов / А.Г. Алексеенко, И.И. Шагурин. – 2-е изд., перераб. и доп. – М. : Радио и связь, 1990. – 496 с. : ил.
3. Жердев М.К. Методика контролю технічного стану аналогових пристроїв з елементами зовнішнього логічного управління / М.К. Жердев, Г.Б. Жиров, П.Ю. Катін // Збірник наукових праць Військового інституту телекомунікацій та інформатизації НТУУ «КПІ». – 2004. – Вип. № 3. – С. 22-33.

РАЗРАБОТКА ПРОВЕРЯЮЩИХ ТЕСТОВ ДЛЯ ДИАГНОСТИРОВАНИЯ АНАЛОГОВИХ УСТРОЙСТВ ДИНАМИЧЕСКИМ МЕТОДОМ

П.А. Шкулипа[1], Н.К. Жердев[2], Г.Б. Жиров[2]

[1] Одесская государственная академия технического регулирования и качества, ул. Ковальская, 15, Одесса, 65020, Украина
[2] Военный институт Киевского национального университета имени Тараса Шевченко, ул. Ломоносова, 81а, Киев, 03680, Украина

Разрабатывается проверяющий тест для аналогового устройства, которое работают как система автоматического управления динамическим методом диагностирования. Это позволяет применить динамический метод диагностирования к широкому классу аналоговых устройств.

Ключевые слова: динамический метод, проверяющий тест, аналоговое устройство

DEVELOPMENT OF TEST PATTERN FOR DIAGNOSING OF ANALOG DEVICES BY DYNAMIC METHODS

Pavel A. Shkulipa[1], Nikolai K. Zherdev[2], Hennadiy B. Jirov[2]

[1] Odessa State Academy of Technical Regulation and Quality, 15 Kovalska str., Odessa, 65020, Ukraine
[2] Military Institute, Taras Shevchenko National University of Kyiv, 81-A Lomonosov str., Kyiv, 03680, Ukraine

Developed test pattern for the analog device, which works as automatic control system, by dynamic method of diagnosing. It allows to apply the dynamic diagnostic method to the wide class of analog devices.

Keywords: dynamic method, test pattern, analog devices

УДК 004.891.3

Informatics and Mathematical Methods in Simulation
Vol. 2 (2012), No. 2, pp. 158-164

ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ МЕТОДУ ПОШУКУ ІНФОРМАЦІЇ ДЛЯ ДІАГНОСТУВАННЯ КОМП'ЮТЕРНИХ СИСТЕМ

І.В. Муляр[1], В.М. Джулій[1], І.В. Пампуха[2], Є.С. Лєнков[3]

[1] Хмельницький національний університет,
вул. Інститутська, 11, Хмельницький, 29016, Україна
[2] Військовий інститут Київського національного університету імені Тараса Шевченка,
вул. Ломоносова, 81а, Київ, 03680, Україна
[3] Київський національний університет імені Тараса Шевченка,
вул. Володимирська, 60, Київ, 01601, Україна

Описується моделювання методу пошуку інформації для діагностування комп'ютерних систем. В результаті експериментальних досліджень встановлено, що запропоновані моделі й алгоритми забезпечують підвищення повноти відповіді при побудові розширеного запиту на 12-16% у порівнянні зі звичайним запитом і підвищення частки виданих системою достовірних документів на 6-8%.

Ключові слова: електронні носії інформації, електронний документообіг, системи діагностування, комп'ютерні системи

Вступ

На сьогодні в різних галузях науки і техніки накопичені величезні об'єми інформації, і темпи їх зростання постійно збільшуються. Цьому сприяють розвиток мережних технологій, зокрема мережі Internet, збільшення літературних джерел, масове поширення електронних носіїв інформації, електронний документообіг, впровадження автоматизованих систем різного призначення та прогресивних інформаційних технологій. Але часто ця різноманітна інформація є надлишковою та слабкоструктурованою. При пошуку діагностичної інформації на сьогодні майже не аналізуються моделі об'єктів діагностування, поверхнево аналізуються методи тестування сучасних комп'ютерних систем (КС), довідникова література, а також надбання автоматизованих систем діагностування, зокрема, їх баз даних та баз знань. Виникають труднощі і при аналізі великих об'ємів мультимедійного наповнення стосовно діагностування КС. Тому розв'язок задачі інформаційного пошуку необхідної інформації у загалі відомої і доступної інформації стає не тільки пріоритетним, а й необхідним для своєчасного доступу до неї.

У теперішній час існує гостра необхідність розроблення методів і засобів інформаційного забезпечення процесу діагностування КС, що в значній мірі знижує ефективність процесу діагностування та його достовірність.

Однією із важливих складових при реалізації систем діагностування КС є організація ефективних процесів пошуку інформаційного забезпечення процесу діагностування. Зазначена проблема особливо актуальна для розподілених виробничих структур, окремі елементи яких територіально роз'єднані й значно віддаленні один від одного. У даний час активно розвивається ціла галузь інформаційних систем, призначених для обробки інформації, зокрема, сучасні довідкові системи, електронні енциклопедії, довідково-правові системи, системи керування документами, системи автоматизації

ділових процесів (*workflow*-системи), комплекси підтримки групової роботи й т.д. Для пошуку інформації, представленої у вигляді документів, використовуються системи автоматизованого пошуку документованої інформації.

Автоматизований пошук діагностичної інформації сприяє обґрунтованому скороченню об'єму інформації, що підвищує оперативність та якість процесу діагностування [1].

Постановка проблеми

Протягом останніх декількох десятків років список задач інформаційного пошуку значно розширився й тепер включає питання моделювання, класифікації й кластеризації документів, проектування архітектури пошукових систем і користувацьких інтерфейсів, мови запитів. Виходячи із необхідності ефективності функціонування сучасних пошукових систем, основними вимогами до них є:

- зручність і повнота подання запитів для користувача – форма вхідного запиту повинна дозволяти легко виражати будь-які вимоги, що відносяться до потрібної інформації, будучи при цьому інтуїтивно зрозумілою і простою у застосуванні;
- точність проведеного пошуку – вся інформація, видавана системою, повинна бути релевантною запиту користувача;
- повнота здійснюваного пошуку – необхідно видавати список, що включає абсолютно всю потрібну інформацію, що відповідає предметній області забезпечення процесу діагностування;
- висока швидкість роботи – час обробки запиту повинен бути мінімальним з урахуванням функціональних можливостей використовуваних засобів обчислювальної техніки.

З метою перевірки працездатності розроблених моделей, алгоритмів і архітектури автоматизованої системи інформаційного забезпечення процесу діагностування [2, 3], а також аналізу одержуваних з використанням запропонованих методів пошуку результатів і порівняння цих результатів з аналогами, необхідно провести експериментальні дослідження методу пошуку діагностичної інформації.

Модель інформаційно-пошукової системи діагностування

При моделюванні системи пошуку діагностичної інформації користувача цікавить насамперед можливість побудови деякої функції, що характеризує поводження об'єкту, що моделюється. Найбільш важливим показником для дослідження будь-якої системи є показник її ефективності. Імітуючи різні реальні ситуації, користувач може оцінити ефективність різних принципів керування системою, порівняти можливі варіанти структури системи, визначити ступінь впливу змін параметрів системи й початкових умов на ефективність. При проектуванні моделі системи інформаційного забезпечення процесу діагностування були виділені наступні етапи:

1) встановлення границь моделювання й вибір показників для порівняння ефективності варіантів системи (в якості таких показників були обрані в першу чергу кількість виданих формально релевантного запиту інформаційного забезпечення і частка істинно релевантного (достовірного) інформаційного забезпечення у числі виданого);

2) складання концептуальної моделі;

3) складання формального опису системи інформаційного забезпечення процесу діагностування – були використані алгоритми, математичні моделі й методи, розроблені в [3];

4) складання опису імітаційної моделі;

5) програмування моделі й налагодження програми;

6) випробовування й дослідження моделі.

Значне число функціональних дій компонент системи інформаційного забезпечення процесу діагностування однакові. Кожна дія може бути представлена у вигляді набору найпростіших операцій, крім того, можлива побудова функціональних залежностей їхнього виконання один від одного. Для імітації поводження подібних систем використовується так званий транзакцій спосіб організації квазіпаралелізму, при якому однотипні функціональні дії об'єднуються. Виникнення тих або інших подій у моделі становлять так звані транзакції – запити на виконання певної групи об'єднаних функціональних дій. Зв'язок між компонентами моделі встановлюється за допомогою системи черг, обраних дисциплін надходження й способів добування з них транзакцій. У будь-який момент часу може виконуватися тільки одна функціональна дія й користувача цікавить вплив цієї дії на поводження всієї системи.

Для опису подібних моделей створюється фіксований набір стандартних блоків обслуговування того або іншого набору функціональних дій. На рис. 1 представлено узагальнену схему функціонування імітаційної моделі функціонування системи інформаційного забезпечення процесу діагностування. Джерелами утворення транзакцій є запити користувачів на пошук інформації. У блоці «поглинач» знищуються всі транзакції, що добралися до нього. Блок обробки запитів сканує списки запитів і створює нові транзакції (запити або дії).

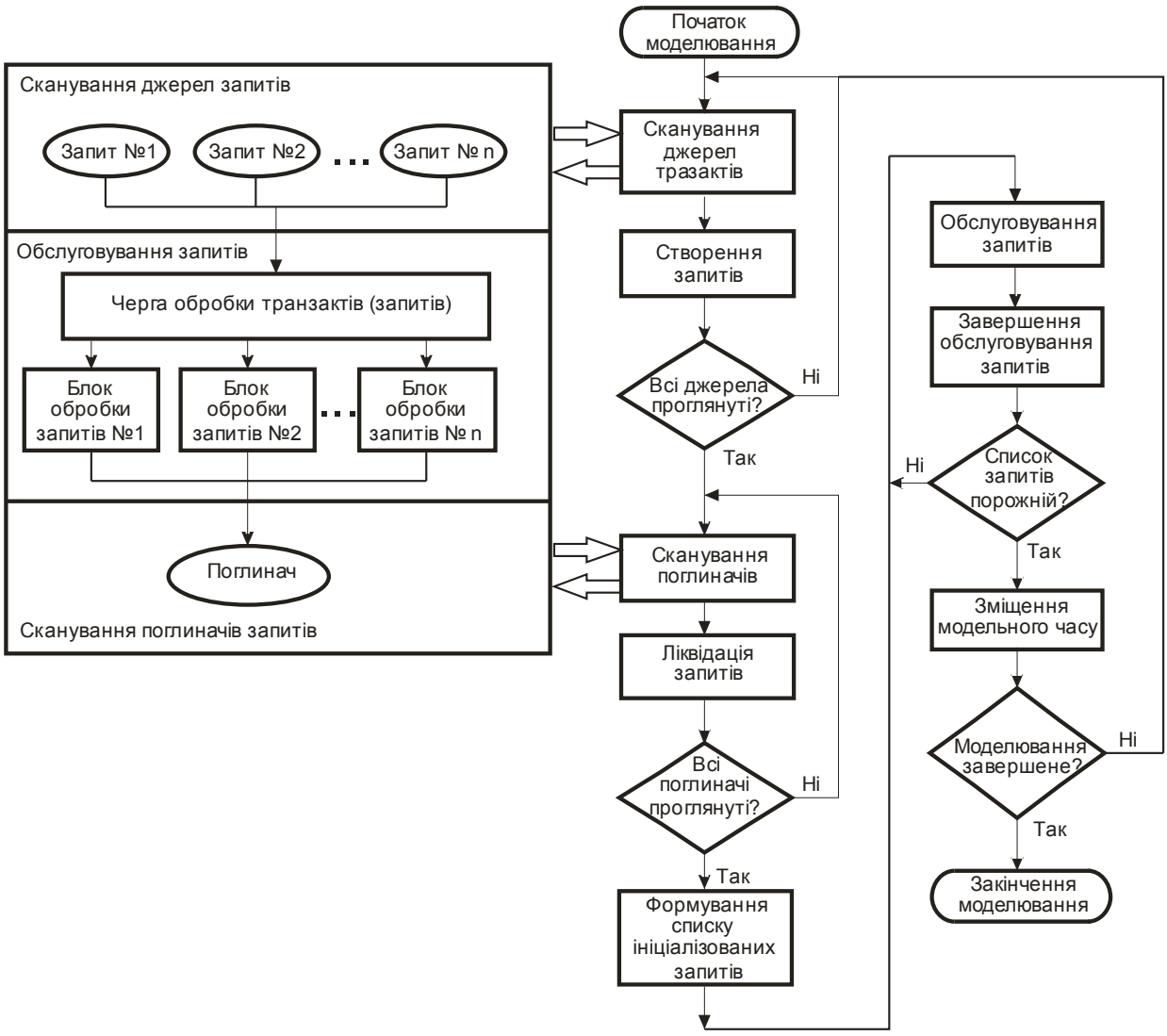


Рис. 1. Модель системи пошуку діагностичної інформації

До складу системи входять лінгвістичні і програмні засоби з відповідними інформаційними файлами: мова спілкування інженера-діагноста з системою; інформаційна (внутрішня) мова системи; транслятор; об'єктно-орієнтована база даних; база знань; керуюча програма; пакети прикладних програм пошуку, формування і актуалізації інформаційної бази.

Відповідно до розробленого алгоритму розроблено програмне забезпечення (рис. 2).

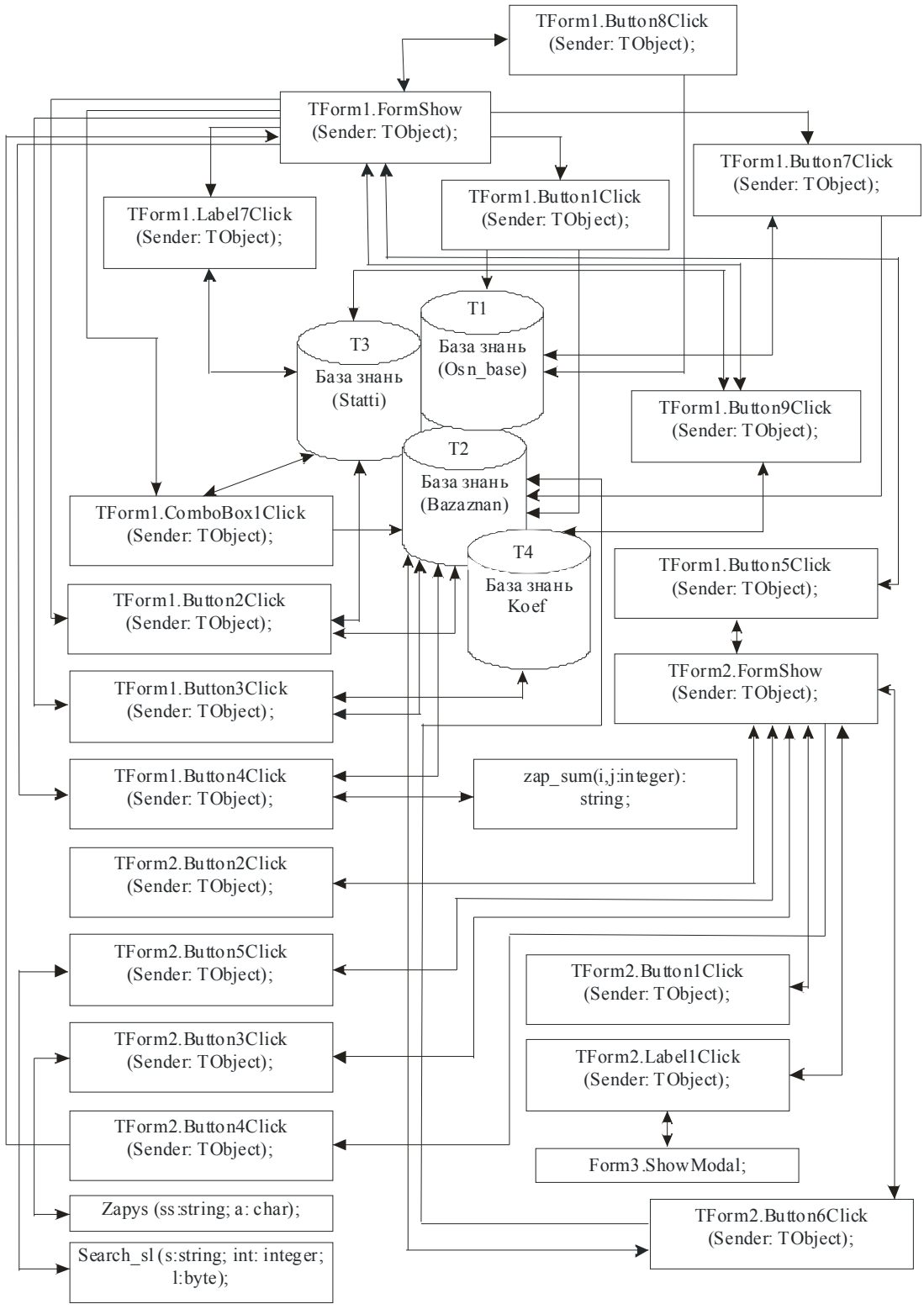


Рис. 2. Блок-схема програмного забезпечення пошуку діагностичної інформацій

Система працює наступним чином. Блок сканування джерел переглядає джерела виникнення запитів на пошук інформації й передає керування моделлю блоку обслуговування запитів. Запити розміщаються в чергу на обробку й у міру функціонування моделі системи надходять у блоки обробки запитів. Потім керування передається блоку перегляду поглиначів, що переглядає черги запитів, які завершили своє перебування в моделі системи й передає керування блоку знищення запитів. Коли переглянуті всі поглиначі, керування передається блоку формування списку ініціалізованих на обробку запитів.

Блок формування списку ініціалізованих запитів переглядає черги запитів і вибирає із них ті, у яких час ініціалізації збігається із поточним, створюючи список активізованих запитів. По закінченні перегляду всіх запитів виробляється перевірка умови «список ініціалізованих запитів порожній». Після закінчення перегляду запитів перевіряється умова закінчення моделювання. Якщо умову закінчення не виконано, то керування передається блоку сканування джерел.

При виконанні умови закінчення моделювання користувачеві видаються його результати. У такий спосіб модель циклічно сканує різні списки запитів і забезпечує їхнє обслуговування відповідними блоками.

З метою оцінки ефективності розробленої методики було проведено порівняння ефективності функціонування змодельованої системи та традиційних інформаційно-пошукових систем у порівнянні з гіпотетичної системою, що знаходить абсолютно всі релевантні даному запиту документи, що знаходяться в базі даних. Порівняння проводилося за двома критеріями – кількість виданих системами релевантних документів і відсоткова частка виданих релевантних документів від загальної кількості виданих у відповідь на запит документів. На рис. 3 представлено порівняння процентної частки достовірних документів виданих пошуковими системами. Як видно з графіка, різні ефективності систем також проявляються по мірі зростання обсягу оброблюваного архіву. При обсязі архіву в 2000 документів частка достовірних документів, знайдених модельованою пошуковою системою, складає 99.4%, проти 98% у системи, що функціонує за традиційною методикою (рис. 4). Зі зростанням обсягу оброблюваного архіву ця різниця також стає більш помітною. Так, при обсязі архіву в 5000 документів, частка достовірних документів, знайдених модельованої системою, складе майже 99%, в той час як традиційна система видає менше 96%.

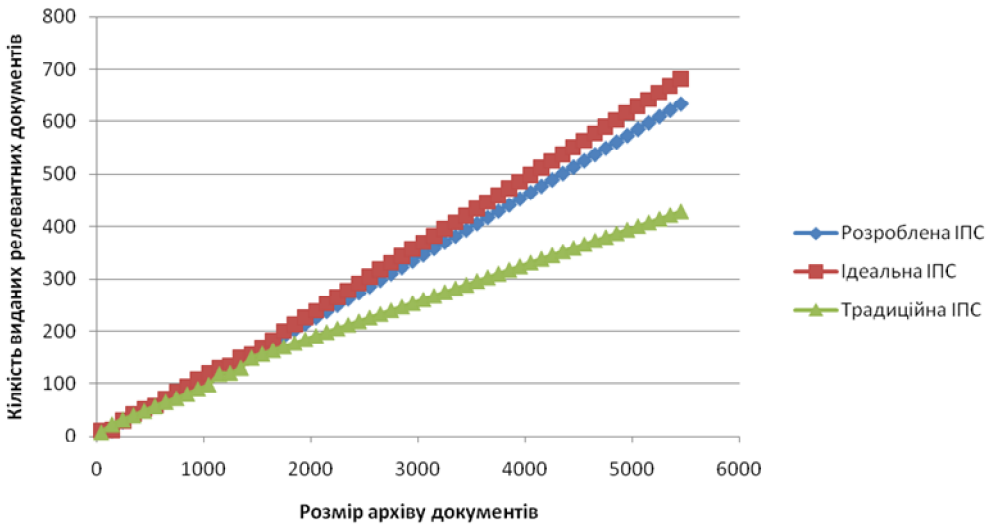


Рис. 3. Кількість виданих релевантних документів

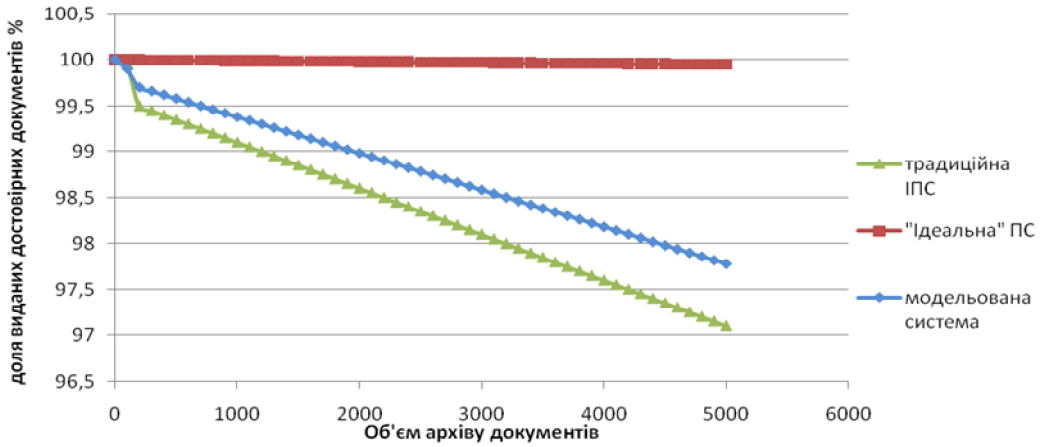


Рис. 4. Частка виданих достовірних документів

Висновки

Для вирішення важкоформалізованої задачі пошуку діагностичної інформації промодельовано метод пошуку діагностичної інформації для тестування КС та їх складових, суть якого полягає у визначенні тих складових тексту (текстів), котрі мають одночасно зв'язки з описом об'єкту діагностування та ознаками, які визначають корисність тексту.

Створено і верифіковано модель пошукової системи в інформаційному просторі забезпечення процесу діагностування на основі розроблених моделей і алгоритмів.

Результати експериментальних досліджень показали, що запропоновані моделі й алгоритми забезпечують підвищення повноти відповіді при побудові розширеного запиту (кількості виданих релевантних документів) на 12-16% у порівнянні зі звичайним запитом і підвищення частки виданих системою достовірних документів на 6-8%. Застосування розробленого методу підвищує ефективність пошуку діагностичної інформації і відповідно процесу діагностування КС та його складових за рахунок зменшення часу на пошук діагностичної інформації (діагностичних програм, описів методів та засобів тестування і таке ін.).

Список літератури

1. Муляр І.В. Імітаційне моделювання процесу пошуку діагностичної інформації / І.В. Муляр // Тези доповідей VI Міжнародної науково-практичної конференції «Військова освіта та наука: сьогодення та майбутнє», 25-26 листопада 2010 р. / Військовий інститут Київського національного університету імені Тараса Шевченка. – К. : [ВІКНУ], 2010. – С. 382-383.
2. Муляр І.В. Модель діагностичних знань в інформаційних системах процесу діагностування пристроїв мікропроцесорних систем / І.В. Муляр, І.В. Пампуха, Є.С. Лєнков // Вісник Східноукраїнського національного університету імені Володимира Даля. Частина 1. – 2010. – №9(151). – С. 85-91.
3. Муляр І.В. Адаптивний метод впорядкування інформаційного забезпечення з використанням пошукової функції / І.В. Муляр // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.:ВІКНУ, 2011. – Вип. №23. – С. 192-196.

ЭКСПЕРИМЕНТАЛЬНЫЕ ИССЛЕДОВАНИЯ МЕТОДА ПОИСКА ИНФОРМАЦИИ ДЛЯ ДИАГНОСТИРОВАНИЯ КОМПЬЮТЕРНЫХ СИСТЕМ

И.В. Муляр[1], В.Н. Джулий[1], И.В. Пампуха[2], Е.С. Ленков[3]

[1] Хмельницкий национальный университет,
ул. Институтская, 11, Хмельницкий, 29016, Украина
[2] Военный институт Киевского национального университета имени Тараса Шевченко,
ул. Ломоносова, 81а, Киев, 03680, Украина
[3] Киевский национальный университет имени Тараса Шевченко,
ул. Владимирская, 60, Киев, 01601, Украина

В статье описывается моделирование метода поиска информации для диагностирования компьютерных систем. В результате экспериментальных исследований установлено, что предложенные модели и алгоритмы обеспечивают повышение полноты ответа при построении расширенного запроса на 12-16% по сравнению с обычным запросом и повышение доли выданных системой достоверных документов на 6-8%.
Ключевые слова: электронные носители информации, электронный документооборот, системы диагностирования, компьютерные системы

EXPERIMENTAL RESEARCH OF INFORMATION RETRIEVAL METHOD FOR DIAGNOSING COMPUTER SYSTEMS

Igor V. Mulyar[1], Volodymyr M. Dzhuly[1], Igor V. Pampukha[2], Eugene S. Lenkov[3]

[1] Khmelnitsky National University
11 Instytutska str., Khmelnitsky, 29016, Ukraine
[2] Military Institute, Taras Shevchenko National University of Kyiv,
81-A Lomonosov str., Kyiv, 03680, Ukraine
[3] Taras Shevchenko National University of Kyiv
64 Volodymyrs'ka str., Kyiv, 01601, Ukraine

The article is devoted to the modeling of the information retrieval method for diagnosing computer systems. As a result of experimental research, found that the proposed models and algorithms provide improved completeness of response when building the advance query by 12-16% in comparison to the ordinary query, and increase the percentage of reliable documents by 6-8%.
Keywords: electronic data carriers, electronic documents circulation, diagnostic systems, computer systems

УДК 519.7

Informatics and Mathematical Methods in Simulation
Vol. 2 (2012), No. 2, pp. 165-172

ПРОГНОЗИРОВАНИЕ ВРЕМЕННЫХ РЯДОВ С ПОМОЩЬЮ ГИБРИДНЫХ МЕТОДОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

В.Г. Пенко

Одесский национальный университет имени И.И. Мечникова,
ул. Дворянская, 2, Одесса, 65082, Украина; e-mail: valerpenko@mail.ru

В статье представлена разработка комплексного подхода к решению задачи прогнозирования одномерных временных рядов, основанного на сочетании нескольких методов, относящихся к категории искусственного интеллекта. Основными компонентами этого подхода являются искусственные нейронные сети и генетический алгоритм. Одним из результатов исследования является разработка программного пакета, результаты тестирования которого на сравнительно небольшом наборе реальных данных подтверждают корректность программной реализации и перспективность предлагаемого гибридного подхода.

Ключевые слова: прогнозирование, временные ряды, искусственные нейронные сети, генетический алгоритм, гибридный подход

Постановка задачи

Прогнозирование временных рядов (ВР) – это классическая прикладная задача, имеющая богатую историю и большое количество предлагаемых методов решения.

В стандартной постановке задачи прогнозирования ВР мы располагаем серией значений некоторого показателя, зафиксированного через равные промежутки времени в прошлом:

$$X_1,\ X_2,\ X_3,\ldots,\ X_n.$$

Как правило, существующие методы претендуют только на достаточно точный краткосрочный прогноз, позволяющий «предсказать» лишь относительно небольшое множество будущих значений.

Обратим внимание на то, что в такой постановке не ставится задача выявить неявно отраженные во временном ряду зависимости целевого показателя от существенных для него значений других характеристик предметной области. Такую задачу можно отнести к задаче так называемого каузального прогнозирования или задаче многофакторного регрессионного анализа.

В отсутствие дополнительной информации задачу прогнозирования ВР пытаются решать, исходя из декомпозиции ВР на следующие составляющие:

$$X = T + S + C + I\ ,$$

где

T – тренд;
S – сезонность;
C – цикличность;

I – случайность.

Упрощенно все количественные методы решения задачи прогнозирования ВР можно разбить на две категории:

1) Статистические методы, использующие некоторую формальную модель и имеющие детерминированную процедуру их применения.

2) Методы, использующие один или несколько универсальных подходов, относящихся к категории подходов искусственного интеллекта.

В свою очередь группа статистических методов насчитывает довольно большое количество эконометрических методов (начиная от «наивных» моделей, заканчивая наиболее сложными в этой категории методами: метод Хольта и Брауна и метод Винтерса).

Наиболее развитыми среди статистических являются методы Бокса-Дженкинса. Это целая группа методов, среди которых, пожалуй, наиболее популярным является метод ARIMA, который в силу своей популярности, встроен практически в любой специализированный пакет для прогнозирования.

Выбор того или иного статистического метода сильно зависит от варианта декомпозиции ВР на трендовую, сезонную, циклическую и случайную составляющую.

В связи с этим, применение подобного подхода к прогнозированию для получения прибыли в глобальной среде современного рынка сталкивается с трудностями, часто объясняемыми так называемым эффективным поведением рынка [1].

Нейросетевые модели считаются перспективными для решения задачи прогнозирования ВР. Потенциальная применимость их для решения задачи прогнозирования ВР основана на теореме Колмогорова о представимости любой произвольной функции от *n* аргументов в виде суммы суперпозиций одномерных непрерывных монотонных функций. Существует несколько публикаций, в которых обоснована модификация этой теоремы в терминах многослойной нейронной сети (НС) с сигмоидальной функцией приспособленности [2].

Таким образом, НС по своей природе не является ориентированной на некоторую модель поведения временного ряда, являясь весьма универсальным средством аппроксимации. Это позволяет рассчитывать на повышение степени автоматизации процесса прогнозирования.

Однако нейросетевая модель не является готовой к употреблению технологией – существует немало проблем, возникающих на всех этапах использования НС: подготовка исходных данных, конструирование конфигурации НС, обучение НС и интерпретация результатов работы НС.

В таких условиях естественным выглядит поиск более эффективных и автоматизированных решений на основе удачного сочетания нескольких различных по своей природе методов. Образно говоря, такие гибридные сочетания позволяют рассчитывать на получение синергетического эффекта от их совместного применения.

В данной работе рассматриваются два довольно универсальных подхода, которые принято относить к категории методов искусственного интеллекта – НС и генетический алгоритм (ГА). Несмотря на большое количество исследований и публикаций, посвященных такому сочетанию, дальнейший поиск перспективных комбинаций в этой области все еще имеет смысл. Это связано с потенциально большим количеством подобных сочетаний. В некоторых публикациях [3] даже делается попытка классифицировать все подобные гибриды.

Целью данного исследования является разработка эффективных методов прогнозирования одномерных временных рядов, обладающих следующими свойствами:

- независимость от ограничений, связанных со структурными особенностями динамической системы, определяющей поведение временного ряда;
- высокий уровень адаптивности в отношении параметров настройки, характерных для нейросетевых и гибридных подходов искусственного интеллекта.

Нейросетевое прогнозирование временных рядов

Практически во всех случаях применения нейросетевого подхода должна быть осуществлена трансформация постановки задачи в концепции используемой для решения модели.

При решении задача прогнозирования ВР с помощью НС такая трансформация обычно выполняется методом «скользящего окна». Этот метод достаточно прост и продемонстрирован на следующем примере.

Допустим, имеется временной ряд из 9 компонент – X_i, $i = \overline{1,9}$.

Выберем «ширину окна» равной 5. Тогда первое окно состоит из элементов $X_1,\ldots,X_5$ и на основании этих данных нужно спрогнозировать следующий элемент X_6. Наш небольшой временной ряд, таким образом, состоит из 4-х скользящих окон, представленных в таблице 1.

Таблица 1.

Последовательность скользящих окон для временного ряда

	Исходный вектор	Тестовое значение для прогноза
1	X_1 X_2 X_3 X_4 X_5	X_6
2	X_2 X_3 X_4 X_5 X_6	X_7
3	X_3 X_4 X_5 X_6 X_7	X_8
4	X_4 X_5 X_6 X_7 X_8	X_9

Такой набор данных может быть использован для создания и обучения многослойной НС прямого распространения. Обычно для обучения таких сетей используют алгоритм обратного распространения ошибки или его модификацию. Фактически способ обучения не имеет большого значения. Основной задачей здесь является достижение приемлемого минимума значения функционала ошибки. Здесь чаще всего используют критерий *Root-Mean-Square* (RMS), однако существуют и другие критерии.

Применение такого подхода к прогнозированию временных рядов вызывает целый ряд вопросов. Основными, на наш взгляд, являются следующие:

1) Как подобрать оптимальную ширину скользящего окна? При наличии четко выраженной цикличности в поведении временного ряда может выявиться существенная зависимость результатов прогнозирования от корреляции между шириной скользящего окна и циклом колебаний временного ряда. Это соображение заставляет считать нейросетевой подход в некоторой степени ориентированным на модель данных, используемую для исследуемого ВР. Теоретическим основанием для решения этой задачи является теорема Такенса, методика применения которой изложена в [4]. Еще более практической является методика *box counting* [5].

2) Как обеспечить актуальность прогнозов? Последовательность значений временного ряда является отражением скрытых зависимостей, значение которых со временем может изменяться (увеличиваться или наоборот, практически полностью исчезать). В этой ситуации необходимо каким-то образом отдавать предпочтение более свежим данным в обучающем множестве. Сделать это можно, внедрив в процесс прогнозирования адаптивную процедуру переобучения, либо снабдить НС обратными связями, тем самым обеспечив ей необходимую «память» о прошлых состояниях.

Входной и выходной слой НС определяются, исходя из параметров скользящего окна – количество нейронов во входном слое равно ширине окна, а в выходном слое – один нейрон, представляющий результат прогнозирования. При таких ограничениях НС может иметь различное количество скрытых слоев с различным количеством

нейронов. Надежных и теоретически обоснованных критериев относительно топологии НС не существует. Чаще всего на практике применяют различные эмпирические правила.

Обучение прогнозирующей нейронной сети

Градиентные методы обучения нейронных сетей отличаются рядом присущих им недостатков, достаточно хорошо описанных в литературе [6]. Чаще всего в этом ряду называют проблему попадания в локальный минимум и переобучение. В связи с этим в данной работе сделана попытка исследовать применимость других подходов к обучению, в меньшей степени «страдающих» упомянутыми проблемами. Поскольку обучение нейронной сети на примерах является частным случаем задачи минимизации, то в поле зрения попадают два перспективных метода, которые принято относить к категории методов искусственного интеллекта:

1) Генетический алгоритм.

2) Группа эволюционных алгоритмов, среди которых выделяется так называемый «алгоритм муравьиной колонии».

Использование для обучения муравьиного алгоритма остается перспективным направлением исследования. В данной работе для обучения сети реализован генетический алгоритм.

Важнейшим элементом ГА является возможность вычислить некоторый обобщенный показатель приспособленности особи в популяции. В нашем случае особью является НС. В рамках процесса отбора НС отличаются друг от друга степенью успешности воспроизведения данных обучающего множества. Часто для оценки этого показателя используют критерий RMS, который для представленной выше совокупности скользящих окон временного ряда выражен формулой (1):

$$\sqrt{\frac{\left(X_6 - X_6'\right)^2 + \left(X_7 - X_7'\right)^2 + \left(X_8 - X_8'\right)^2 + \left(X_9 - X_9'\right)^2}{4}} \qquad (1)$$

Следует обратить внимание на то, что комбинация ГА+НС является чрезвычайно популярной и существует в большом количестве разновидностей. Позже в данной работе будет предложен оригинальный на наш взгляд, подход к использованию генетического алгоритма для оптимизации значений глобальных параметров настройки всего процесса прогнозирования. В качестве примера, к таким глобальным параметрам можно отнести ширину скользящего окна.

Подобная идея использования генетического алгоритма на более высоком композиционном уровне изучения модели приводит к существенному увеличению вычислительной сложности таких экспериментов. Поэтому, применяя для оптимизации генетический алгоритм, мы должны уделить критическое внимание показателям его быстродействия и точности.

Особенности генетического алгоритма

В связи с требованиями, предъявляемыми к генетическому алгоритму в контексте решаемой задачи, рассмотрим две основные возможности:

- ГА с вещественным кодированием в хромосомах всей совокупности синаптических весов НС;
- кодирование параметров, связанных с топологией нейросети.

Генетический алгоритм с вещественным кодированием. Применение ГА для обучения НС предполагает определенный способ кодирования особей. Целью обучения

является получение такой конфигурации нейронной сети, которая обеспечит приемлемое значение функционала ошибки. В нашем исследовании мы зафиксируем топологию сети. Иначе говоря, количество слоев и нейронов в каждом слое будет выбираться эвристически либо определяться некоторым целенаправленным образом, но за пределами процедуры обучения нейросети. В таком случае одним из естественных способов представления нейросети является упорядоченное множество значений синаптических весов, сохраняющее связь между его элементами и расположением соответствующего синапса в сети.

Предлагаемое в классическом случае бинарное кодирование признаков в структуре хромосомы влечет за собой определенные трудности при выполнении поиска в непрерывных пространствах, связанные с быстрорастущей размерностью пространства поиска. Допустим, для фенотипа из 100 признаков, изменяющихся в интервале [-500; 500], требуется найти минимум с точностью до шестого знака после запятой. В этом случае при использовании ГА с двоичным кодированием длина хромосомы составит 3000 элементов, а пространство поиска – около 10^{1000}.

В данной работе реализован генетический алгоритм с вещественным кодированием синаптических весов (РГА). Помимо понижения размерности пространства поиска генетический алгоритм с вещественным кодированием позволяет повысить точность найденных решений и скорость нахождения оптимального решения (из-за отсутствия процессов кодирования и декодирования хромосом на каждом шаге алгоритма).

Естественно, что для такого подхода не подходят стандартные генетические операторы. В связи с этим были разработаны и исследованы специальные операторы. Довольно подробный их обзор приведен в [7].

Вещественный кроссовер. Обозначим две хромосомы, выбранные оператором селекции для проведения кроссовера как $C_1 = \left(c_1^1, c_2^1, \ldots, c_n^1\right)$ и $C_2 = \left(c_1^2, c_2^2, \ldots, c_n^2\right)$.

▪ *Плоский кроссовер.* Потомок $H = \left(h_1, h_2, \ldots, h_n\right)$, где h_i – случайное число из интервала $\left[c_i^1, c_i^2\right]$.

▪ *Арифметический кроссовер.* Создаются два потомка $H_1 = \left(h_1^1, h_2^1, \ldots, h_n^1\right)$ и $H_2 = \left(h_1^2, h_2^2, \ldots, h_n^2\right)$, гены которых образуются по следующим законам:

$$h_i^1 = \eta c_i^1 + (1-\eta) c_i^2,$$

$$h_i^2 = \eta c_i^1 + (1-\eta) c_i^1,$$

$$i = \overline{1,n},$$

где $\eta \in [0,1]$ – константа.

▪ *BLX-α кроссовер.* Генерируется один потомок $H = \left(h_1, h_2, \ldots, h_n\right)$, где h_i – случайное число из интервала $\left[c_{\min} - \Delta\alpha, c_{\max} + \Delta\alpha\right]$, $c_{\max} = \max\left(c_i^1, c_i^2\right)$, $c_{\min} = \min\left(c_i^1, c_i^2\right)$, $\Delta = c_{\max} - c_{\min}$.

▪ *Линейный кроссовер.* Создаются три потомка, рассчитываемые по формулам:

$$h_i^1 = \frac{c_i^1 + c_i^2}{2}, \quad h_i^2 = \frac{3c_i^1 + c_i^2}{2}, \quad h_i^3 = \frac{-c_i^1 + 3c_i^2}{2}, \quad i = \overline{1,n}.$$

Наиболее эффективным оператором скрещивания признан *BLX*-кроссовер с $\alpha = 0.5$. Особенность данного оператора в том, что при скрещивании генов значения

потомка могут лежать в некоторой области, выходящей за границы значений этих генов на величину $\Delta\alpha$.

Вещественная мутация. В качестве оператора мутации наибольшее распространение получили случайная и неравномерная мутация Михалевича.

При случайной мутации ген, подлежащий изменению, принимает случайное значение из интервала своего изменения

В публикациях, посвященных РГА, высказывается сомнение в его эффективности. Одной из задач данной работы является проверка этих утверждений.

Программная реализация прогнозирующей системы

Изложенные выше элементы подхода к прогнозированию временных рядов были реализованы в виде Windows-приложения с использованием объектно-ориентированных возможностей языка C#. В настоящий момент главное окно этого приложения (уже после обучения нейронной сети) представлено на рис. 1:

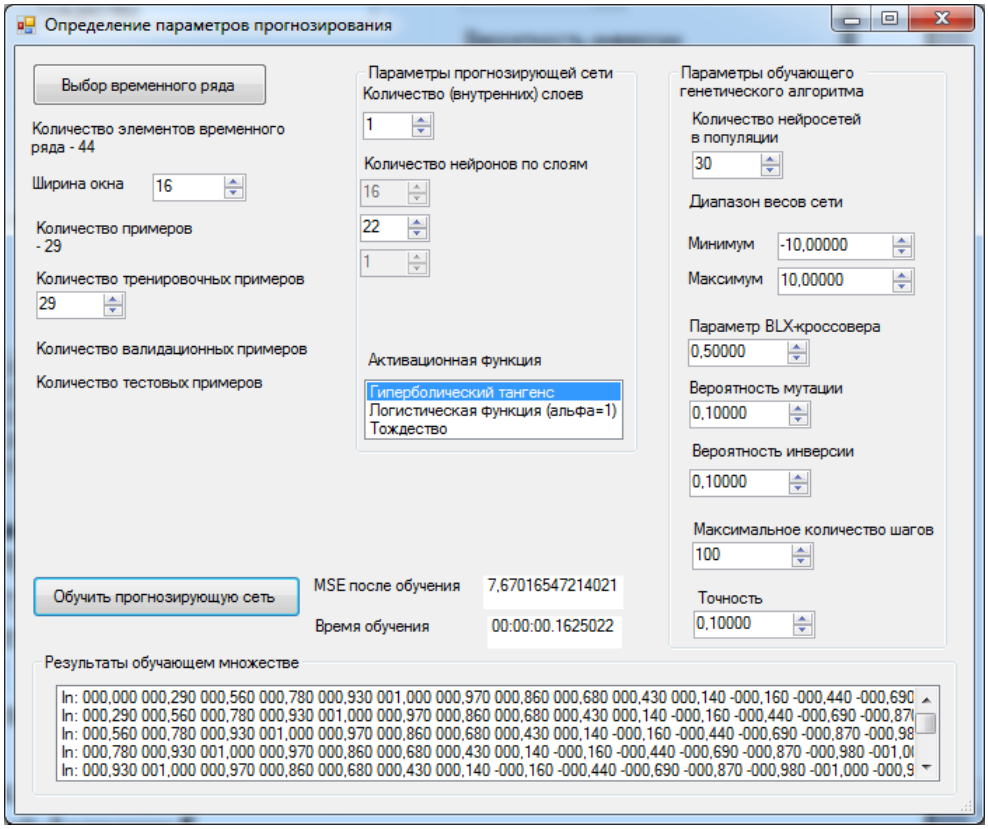


Рис. 1. Главное окно разработанного программного приложения

Таким образом, мы видим, что приложение предлагает пользователю возможность определения целого ряда структурных и параметрических характеристик ВР, НС и ГА для ее обучения:

- ширина скользящего окна;
- количество тренировочных примеров;
- количество слоев НС;
- количество нейронов на каждом внутреннем слое;
- разновидность активационной функции;
- количество НС в популяции;
- диапазон весов в НС;

- параметр BLX-кроссовера;
- вероятность мутации;
- вероятность инверсии.

В эксперименте использовались данные о ВВП США, доступные на сайте «*The World Bank*» [8].

Процесс обучения выполняется довольно быстро (в примере, показанном на рис. 1 оно составило 0.16 сек. для 100 итераций цикла ГА). При этом достигается значение RMS, равное 7.67.

Для сравнения качества и быстродействия сходный эксперимент производился в среде MATLAB. Хотя MATLAB поддерживает помимо НС и генетический алгоритм, представляло интерес сравнение сочетания ГА и НС с НС, обучающимися одним из наиболее быстрых градиентных методов (метод Левенберга-Маркара). В ходе эксперимента в аналогичных условиях выявились сравнимые показатели быстродействия и точности (значение RMS 3.75 было достигнуто за 0.1 сек.) Следует отметить некорректность непосредственного сравнения подобного рода. Дело в том, что в процедуру обучения НС в MATLAB встроена автоматизированная методика определения корректного момента завершения (во избежание переобучения сети), которая основана на использовании трех подмножеств в обучающем множестве. Способ выделения этих подмножеств представляется не совсем корректным в контексте задачи прогнозирования ВР, поскольку более поздние элементы временного ряда, скорее всего более актуальны для прогнозирования.

Результаты и перспективы

Текущие результаты исследования можно подытожить следующим образом:

1) Рассмотрены элементы гибридного подхода к прогнозированию ВР.

2) Хотя большинство из элементов предлагаемого подхода рассматривались в различных информационных источниках, их комплексное применение является вполне оригинальным.

3) Разработан программный инструмент, демонстрирующий корректную работу на небольшой выборке временных рядов и открывающий возможность дальнейших экспериментальных исследований с целью выявления дополнительных закономерностей.

4) Определены настроечные параметры, влияющие на корректность и эффективность прогнозирования.

Наиболее перспективной возможностью является автоматизированная оптимизация параметров сети и генетического алгоритма – с помощью того же генетического алгоритма. Другая возможность заключается в использовании специализированного кодирования параметров нейронной сети, которое ориентировано на топологию сети.

Список литературы

1. Мандельброт Б. (Не)послушные рынки [Текст] : фрактальная революция в финансах / Б.Х. Мандельброт, Р.Л. Ричард ; пер. А.Ю. Заякин. – М. : Вильямс, 2006. – 389 с.
2. Cybenko G. Approximation by Superpositions of a Sigmoidal Function / G. Cybenko // Mathematics of Control, Signals, and Systems. –1989. – Vol.2, No.4. – PP. 303-314.
3. Рутковская Д. Нейронные сети, генетические алгоритмы и нечеткие системы [Текст] / Д. Рутковская [и др.] ; пер. с пол. И.Д. Рудинский. – М. : Горячая линия-Телеком, 2007. – 383 с.
4. Нелинейные эффекты в хаотических и стохастических системах / В.С. Анищенко, В.В. Астахов, Т.Е. Вадивасова и др. – Москва-Ижевск: ИКС, 2003. – 530 с.
5. Ежов А.А. Нейрокомпьютинг и его применения в экономике и бизнесе [Текст] / А.А. Ежов, С.А. Шумский. – М. : [б. в.], 1998. – 222 с.

6. Хайкин С. Нейронные сети: полный курс / Хайкин С.; пер. с англ. – [2-е изд., испр.]. – М.: Вильямс, 2006. – 1104 с.
7. Herrera F. Tackling Real-Coded Genetic Algorithms: Operators and Tools for Behavioural Analysis / F. Herrera, M. Lozano, and J.L. Verdegay // Artificial Intelligence Review. – 1998. – Vol.12, No.4. – PP. 265-319.
8. Data: The World Bank *[Електронний ресурс]* // The World Bank. Washington, USA. Режим доступу: http://data.worldbank.org (Дата звернення: 26.07.2012).

ПРОГНОЗУВАННЯ ЧАСОВИХ РЯДІВ ЗА ДОПОМОГОЮ ГІБРИДНИХ МЕТОДІВ ШТУЧНОГО ІНТЕЛЕКТУ

В.Г. Пенко

Одеський національний університет імені І.І. Мечникова,
вул. Дворянська, 2, Одеса, 65082, Україна; e-mail: valerpenko@mail.ru

У статті представлена розробка комплексного підходу до вирішення задачі прогнозування одновимірних часових рядів, заснованого на поєднанні декількох методів, що відносяться до категорії штучного інтелекту. Основними компонентами цього підходу є штучні нейронні мережі і генетичний алгоритм. Одним з результатів дослідження є розробка програмного пакета, результати тестування якого на порівняно невеликому наборі реальних даних підтверджують коректність програмної реалізації і перспективність запропонованого гібридного підходу.
Ключові слова: прогнозування, часові ряди, штучні нейронні мережі, генетичний алгоритм, гібридний підхід

TIME SERIES FORECASTING BY HYBRID ARTIFICIAL INTELLIGENCE METHOD

Valery G. Penko

Odessa I.I.Mechnikov National University,
2 Dvoryanskaya str., Odessa, 65082, Ukraine; e-mail: valerpenko@mail.ru

The paper presents an integrated approach to the problem of one-dimensional time-series forecasting, based on a combination of several methods relates to the category of artificial intelligence. The main components of this approach is an artificial neural network and genetic algorithm. A software package which was developed as one result of study demonstrates correct results on a relatively small set of real data. It confirms the correctness of the program implementation and the prospects of the proposed hybrid approach.
Keywords: forecasting, time series, artificial neural networks, genetic algorithm, hybrid approach

УДК 519.852: 004.424.27.021

Informatics and Mathematical Methods in Simulation
Vol. 2 (2012), No. 2, pp. 173-179

ОБОБЩЕНИЕ АЛГОРИТМОВ МЕТОДА ВЕТВЕЙ И ГРАНИЦ ДЛЯ РЕШЕНИЯ ЗАДАЧ ЛИНЕЙНОГО ПРОГРАММИРОВАНИЯ С БУЛЕВЫМИ ПЕРЕМЕННЫМИ

Б.И. Юхименко

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: pm1987pm@gmail.com

В работе проведен анализ и предложен способ увеличения скорости сходимости алгоритмов метода ветвей и границ путем расширения атрибутики метода за счет введения понятия функции предпочтения. Рассмотрены два типа функций предпочтения: обычные и рандомизированные. Показано, что рандомизированные функции предпочтения приводят к лучшему результату в смысле вычислительной сложности, особенно с учётом длины частичного решения.

Ключевые слова: целочисленное линейное программирование, метод ветвей и границ, функция предпочтения

Введение

Дискретная оптимизация, как достаточно новый математический аппарат, широко используется для принятия решений в различных областях деятельности человека. Сферы применения этой науки не ограничиваются математическим моделированием в организационном управлении. Дискретные задачи возникают в транспорте, при решении самых различных задач в распределении – размещении неделимых объектов, в задачах о покрытии на графах и во многих других проблемах, вплоть до организации компьютерных интернет-сетей.

Что касается методов решения таких задач, то основное внимание уделяется решению отдельной части дискретных задач – задачам целочисленного линейного программирования (ЦЛП). Хорошо известно, что методы решения задач ЦЛП делятся на три основных класса: метод отсекающих плоскостей, метод ветвей и границ и приближения, эвристический метод. Компьютерная их реализация для широкого пользователя сконцентрирована на методах Гомори (отсекающих плоскостей). Комбинаторные методы (методы ветвей и границ) программно менее реализованы, хотя их легко можно модифицировать для конкретного случая решения прикладной задачи, учитывая её специфическую структуру в математической модели, а также специфику фактической исходной информации. Методы ветвей и границ легко модифицируются при превращении их из точных в приближенные методы. Ещё один позитивный момент этого класса методов состоит в том, что логическая их структура несложная, легко реализуемая программно, и вычислительная сложность предопределяется числом итераций. Именно этот момент вызывает необходимость обратить особое внимание на скорость сходимости алгоритмов метода.

Цель статьи и постановка исследования

Целью работы является анализ и увеличение скорости сходимости алгоритмов метода ветвей и границ.

Для достижения цели в работе решаются *задачи*

- расширения атрибутики метода ветвей и границ за счет введения понятия функции предпочтении;
- предлагается ряд функций предпочтения, способствующих увеличению скорости сходимости алгоритмов метода ветвей и границ.

Основная часть

Атрибутика метода ветвей и границ состоит из следующего:

- оценка множества вариантов – число, показывающее, что значение целевой функции для любого варианта из множества не может быть лучше (меньше или больше) чем данное число;
- ветвление – разбиение множества вариантов на подмножества. Это процедура выбора параметра, на основе которого множество вариантов разбивается на ряд подмножеств;
- признак оптимальности – средство, предопределяющее, что лучше найденного варианта не существует во множестве вариантов.

Все эти три момента предопределяют скорость сходимости алгоритмов метода. При алгоритмизации метода от способа оценки множества вариантов требуется, что бы она как можно была бы приближена к значению целевой функции для локального оптимального варианта. Такое требование диктует сам признак оптимальности метода. Однако чем точнее получается оценка, тем вычислительная сложность алгоритма больше. Часто приходится «жертвовать» точностью за счёт упрощения процедуры получения оценок. Вычислительная сложность уменьшается, но увеличивается число итераций при получении оптимального варианта. Частичный перебор вариантов несколько приближается к полному перебору, что не желательно, в особенности для задач большой размерности.

Что касается разбиения множества вариантов на подмножества, то очень важно подобрать параметр, разделяющий варианты на подмножества. В алгоритме Лэнда и Дойга, как бы исключаются из рассмотрения нецелочисленные значения компоненты вектора решений в области её возможного оптимального значения.

При последовательном построении решений [1] параметром деления является конкретизация значений определённой, выбранной каким-то образом компоненты. В задачах линейного программирования с булевыми переменными это осуществить достаточно просто. Если конкретизации подлежит компонента X_{j0}, то множество вариантов делится на два подмножества, одно из которых содержит все варианты, в которых $X_{j0} = 1$.

Сущность признака оптимальности состоит в том, что если получен вариант решения, то следует удостовериться, что, во-первых, ни одно из имеющихся подмножеств не содержат лучше варианта и, во-вторых, что в подмножестве, которому принадлежит проверяемый на оптимальность вариант, не существует варианта лучше, чем проверяемый. Первое требование признака оптимальности очевидное: подмножество, содержащее проверяемый вариант, должно иметь наилучшую по значению оценку, так как при дальнейшем разбиении на более мелкие подмножества значение ни оценки, ни тем самым, значение целевой функции не улучшается. Второй момент – второе требование очень чувствительное по отношению к точности оценки подмножества. Требование совпадения значения целевой функции проверяемого на

оптимальность варианта со значением оценки возможно, в основном, только тогда, когда оценка достаточно точно получена (имеется ввиду, близко к значению целевой функции).

Если полученный вариант не удовлетворяет признаку оптимальности, необходимо продолжить поиск оптимального варианта. Ставится вопрос, какому подмножеству отдать предпочтение. По логике вещей, выбирается подмножество с наилучшей оценкой и продолжается чередование получения оценок с разбиением множества на более мелкие подмножества в поиске лучшего варианта. Опять таки, рассматривая логически, более лучшие (большие в задачах максимизации и меньшие в задачах минимизации) оценки имеют те подмножества, в которых больше количество вариантов. При последовательном построении решения – это подмножество, содержащее меньшее количество конкретизированных переменных – компонент вектора решений.

Предполагается расширить атрибутику метода ветвей и границ ещё одним понятием – функция предпочтения. Функция предпочтения – это способ выбора подмножества, не подвергавшегося разбиению, по определённым правилам, базирующимся на величине оценок.

Рассмотрим более распространенные и проверенные способы оценивания, ветвления, а так же предположим рад функций предпочтения, которые, на наш взгляд, как-то должны способствовать увеличению скорости сходимости алгоритмов метода ветвей и границ.

Итак, пусть имеется задача линейного программирования с булевыми переменными в постановке

$$Z = \max \sum_{j=1}^{n} c_j x_j , \tag{1}$$

при ограничениях

$$\sum_{j=1}^{n} a_{ij} x_j \le b_i , \quad i = \overline{1,m} ; \tag{2}$$

$$0 \le x_j \le 1 , \quad j = \overline{1,n} ; \tag{3}$$

$$x_j \in Z , \quad j = \overline{1,n} , \tag{4}$$

где Z – множество целых чисел.

Область определённости задачи, задаваемая требованиями (2)-(4) расширяется путём отбрасывания требований (4). Задача в постановке (1)-(3) является соответствующей задачей линейного программирования по отношению к задаче целочисленного линейного программирования в постановке (1)-(4). Очевидно, это экстремальное значение целевой функции $Z(x)$ для x из области определённости (2)-(3) всегда будет не хуже экстремального значения $Z(x)$, когда x из области определённости (2)-(3)-(4). Можно утверждать, что получение оценки множества целочисленных вариантов можно осуществить путём решения соответствующей задачи линейного программирования. Методы решения задач линейного программирования не подлежат обсуждению.

Известно [2], что процедуру получения оценок множества целочисленных вариантов можно привести к решению m нецелочисленных задач о ранце. Решаются задачи в постановках

$$Z_i = \max \sum_{j=1}^{n} c_j x_j \,, \tag{5}$$

при ограничениях

$$\sum_{j=1}^{n} a_{ij} x_j \le b_i \,, \tag{6}$$

$$0 \le x_j \le 1 \,, \quad j = \overline{1,n} \,; \tag{7}$$

когда $i = \overline{1,m}$, т.е. имеется общая целевая функция (5) для всех задач, а основные ограничения типа (2) берутся по одной, составляя задачу о ранце.

Оценка множества целочисленных вариантов $Z(x)$ ограничивается сверху значением $Z_{i_0}(x)$, где

$$Z_{i_0}(x) = \min_{i=\overline{1,m}} Z_i$$

Рассмотрим некоторые способы осуществления процедуры ветвления, используя идею последовательного построения решения. В данном случае конкретизируются значения переменных, переходя от одного яруса в дереве решений к другому. Можно сказать, что вектор решений, как бы собирается в процессе ветвления. И так, пусть величина k предопределяет количество конкретизированных переменных, значения которых фиксируются в частичном решении δ^k, а номера компонентов записывают во множестве I_x^k. И так $I_x^k = \{ j \mid x_j \textit{ конкретизировано} \}$. К примеру, если $I_x^3 = \{3,4,6\}$, а $\delta^3 = \{0,1,0\}$, то это значит, что $x_3 = 0$, $x_4 = 1$, $x_6 = 0$; а остальные компоненты пока не зафиксированы.

Известны [3] и экспериментально оценены [4] два способа выбора конкретизируемых переменных. Первый из них руководствуется лексикографической последовательностью переменных вектора решений. Первым конкретизируется x_1, вторым – x_2 и т.д. Второй способ навеян идеями алгоритма Балаша [6] и учитывает величину «вклада» переменной в значение целевой функции и величину неувязки в системе ограничений. Предположим, что имеет частичное решение длины k. Обозначаем его через δ^k и соответствующее множество индексов конкретизированных переменных I_x^k. Тогда вектор ограничений, состоящий из компонент b_i на $(k+1)$ шаге конкретизации определяется так:

$$b_i^k = b_i - \sum a_{ij} x_j \,,$$

$$i = \overline{1,m} \,, \quad j \in I_x^k \,, \quad x_j \in \delta_k \,.$$

На основании величин b_i^k определяется, так называемое, множество «хороших» компонент, компонент, которые могут ещё принимать значение «1».

$$V_j^s = \left\{ \frac{j}{b_i^k - a_{ij}} \geq 0 \right\}, \quad j \notin I_x;$$

где s предопределяет номер итерации (см. ниже).

Далее оцениваются все компоненты, номера которых находятся во множестве V_j^s, а именно определяется P_j согласно формуле:

$$P_j = \sum_{i=1}^{m} \left(b_i^k - a_{ij} \right) \times \sqrt{\frac{C_j}{\min\limits_{j \in V_j^s} C_j}}, \quad j \in V_j^s.$$

Предположим, что $P_{j_0} = \max\limits_{j \in V_j^s} P_j$. Тогда конкретизации подлежит компонента с номером j_0. Формируется множество $I_x^{k+1} = \left\{ I_x^k V_{j_0} \right\}$ и два частичных решения

$$\delta_{k+1}^0 = \left\{ \delta_k \cup \left(x_{j_0} = 0 \right) \right\} \quad \text{и} \quad \delta_{k+1}^1 = \left\{ \delta_k \cup \left(x_{j_0} = 1 \right) \right\}.$$

Оцениваются подмножества, содержащие частичные решения δ_{k+1}^0 и δ_{k+1}^1 по выше предложенной методике и подмножество с лучшей оценкой выбирается для дальнейшего разбиения. Другими словами определяется частичное решение δ_{k+1}. Если окажется, что $V_j^s = \varnothing$, то все неконкретизированные компоненты частичного решения определяются как нулевые, частичное решение становится вариантом решения и проверяется на оптимальность. Если вариант окажется не оптимальным, то необходимо выбрать вершину дерева решений, которая не подвергалась разбиению, возможно, содержит оптимальное решение и, быстрее всего, приведёт к нему или убедимся, что оптимального решения в данном подмножестве не имеется. Ставится вопрос, какой вершине в дереве отдать предпочтение. Выбор определяется алгоритмически при помощи некоторых функций, основанных на величине оценок, длине частичного решения и называемых функциями предпочтения [5].

Рассматриваются два типа функций предпочтения: обычные функции и рандомизированные. Обычные функции – это правило выбора вершины, осуществляется либо по максимальному значению оценки либо по максимальному количеству конкретизированных переменных вектора решений. Выбор вершины с максимальной оценкой – это классический приём. Что касается выбора согласно величине «заполненности» частичного решения, то, во-первых, вычислительная сложность уменьшается при доведении частичного решения до варианта решения задачи, либо к убеждению, что в данном направлении нет оптимального варианта, просмотр следует остановить. Во-вторых, эффект (в смысле вычислительная сложность) возможен за счёт уменьшения просматриваемых вершин.

При использовании рандомизированных функций предпочтения для выбора вершины в дереве, включается элемент случайности. Выбирается определённое количество вершин с наибольшими значениями оценок подмножеств вариантов, их значения приводятся к шкале, определяемого интервалом $(0,1)$, который делится на участки, соответствующие относительной величине оценок. Генерируется значение случайной величины равномерно – распределённой из интервала $(0,1)$. Соответствие значения полученной случайной величины участку интервала, предопределяет вершину дерева решений, с которой необходимо продолжить поиск. Итак, подлежит рассмотрению:

1) обычная функция предпочтения – выбор вершины осуществляется согласно максимальному значению оценок среди:

- всех вершин, не подвергавшихся разбиению;
- среди вершин, не подвергавшихся разбиению и содержащих частичное решение длины не меньше r;

2) рандомизированные функции предпочтения – выбор вершины осуществляются случайно среди:

- k не подвергавшихся разбиению вершин и имеющих наибольшие оценки;
- k не подвергавшихся разбиению вершин с наибольшими оценками и содержащих частичное решение длины не меньше r.

Величина k и r могут варьироваться и иметь самую различную величину.

Заключение

По результатам проведенного эксперимента можно сделать следующий вывод: рандомизированные функции предпочтения приводят к лучшему результату в смысле вычислительной сложности, особенно с учётом длины частичного решения. В настоящий момент усилия авторов направлены на поиск новых типов функций предпочтения.

Список литературы

1. Михалевич В.С. Последовательные алгоритмы оптимизации и их применение. I. II. / В.С. Михалевич // Кибернетика. – 1965. − №1. – С. 45-55; №2. – С. 85-88.
2. Юхименко Б.И. Разработка и обоснование некоторых схем и методов дискретной оптимизации в автоматизаци Михалевич В.С. Последовательные алгоритмы оптимизации и их применение. I. II. / В.С Михалевич // Кибернетика. – 1965. − №1. – С. 45-55; №2. – С. 85-88. и функций распределения – размещения в АСУ: Автореферат диссертации на соискание учёной степени кандидата экономических наук. – Киев, 1982. – 20 с.
3. Юхименко Б.И. Ускоренный алгоритм метода ветвей и границ для решения задачи целочисленного линейного программирования // Труды Одесского политехнического университета. – 2004. – Вып. 2. – С. 223-226.
4. Юхименко Б.И. Сравнительная характеристика алгоритмов метода ветвей и границ для решения задач целочисленного линейного программирования / Б.И. Юхименко, Ю.Ю. Козина // Труды Одесского политехнического университета. – 2005. – Вып. 2. – С. 199-204.
5. Юхименко Б.И. Об эффективности функций предпочтения в алгоритмах целочисленного линейного программирования // Литовский математический сборник. – Вильнюс, 1983. – Том 23, № 1. – С. 134-140.
6. Balas E. An Additive Algorithm for Solving Linear Programs with Zero-One Variables // Operations Research. – 1965. – Vol.13, Num.4. – PP. 517-546.

УЗАГАЛЬНЕННЯ АЛГОРИТМІВ МЕТОДУ ГІЛОК І МЕЖ ДЛЯ РІШЕННЯ ЗАДАЧ ЛІНІЙНОГО ПРОГРАМУВАННЯ З БУЛЕВИМИ ЗМІННИМИ

Б.І. Юхименко

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: pm1987pm@gmail.com

В роботі проведено аналіз та запропоновано спосіб збільшення швидкості збіжності алгоритмів методу гілок і меж шляхом розширення атрибутики методу за рахунок введення поняття функції переваги. Розглянуто два типи функцій переваги: звичайні та рандомізовані. Показано, що рандомізовані функції переваги приводять до кращого результату в сенсі обчислювальної складності, особливо з урахуванням довжини часткового рішення.
Ключові слова: цілочисельне лінійне програмування, метод гілок і меж, функція переваг

GENERALIZED BRANCH AND BOUND ALGORITHM FOR SOLVING LINEAR BOOLEAN PROGRAMMING PROBLEMS

Birute I. Yukhimenko

Odessa National Polytechnic University,
1 Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: pm1987pm@gmail.com

Proposed method for increasing the convergence speed of the branch-and-bound algorithm by introducing the concept of preference functions. Described two types of preference functions – common and randomized. According to factual evidence randomized preference functions lead to a better result in sense of computational complexity, especially considering the length of the partial solution.
Keywords: integer linear programming, branch and bound, preference function

УДК 621.39: 004.7

Informatics and Mathematical Methods in Simulation
Vol. 2 (2012), No. 2, pp. 180-192

УНІВЕРСАЛЬНА РОЗГОРТАЮЧА СІТЬ ПЕТРІ

Д.А. Зайцев[1], Жи Ву Лі[2], Ліанг Хонг[2]

[1] Міжнародний гуманітарний університет,
Фонтанська дор., 33, Одеса, 65009, Україна; e-mail: zsoftua@yahoo.com
[2] School of Electro-Mechanical Engineering, Xidian University,
2 South TaiBai Road, Xi'an, 710071, China; e-mail: systemscontrol@gmail.com

Розроблено універсальну розгортаючу сіть Петрі, яка для довільної заданої ординарної сіті Петрі будує скінчений префікс процесу розгалуження. Розроблено шифрування сіті Петрі та процесу розгалуження певною кількістю цілих невід'ємних чисел, які подано як позиції універсальної розгортаючої сіті, та низку підсітей для роботи із шифрами. Використані основи парадигми обчислень на сітях Петрі із програмування на мові інгібіторних сітей Петрі через композицію підсітей, які подають основні операції та оператори.

Ключові слова: розгортання сітей Петрі, процес розгалуження, універсальна сіть Петрі, парадигма обчислень на сітях Петрі

Вступ

Сіті Петрі [1, 2] та їх різновиди ресурсно-процесних [3, 4] сітей є відомим засобом моделювання виробничих процесів та планування робіт [2, 3]. Але ж пошук ефективних методів аналізу сітей та примусового надавання ідеальних властивостей є занадто актуальним у реальному, особливо великомасштабному виробництві.

Теоретичні методи дослідження властивостей сітей Петрі [1-3] містять побудову та аналіз простору станів (графу досяжних маркувань), алгебраїчні методи розв'язання фундаментального рівняння та застосування лінійних інваріантів позицій та переходів, методи знаходження сифонів та пасток на основі логічних рівнянь, допоміжні методи еквівалентних перетворень, редукції та декомпозиції.

В загальному випадку граф досяжних маркувань є нескінченним [1], що зумовило розробку додаткових скінчених структур таких, як граф (дерево) покривних маркувань. Але граф покривних маркувань може мати достатньо великий розмір для порівняно малих моделей, що заважає його практичному застосуванню в аналізі систем. Проблема відома під назвою вибуху простору станів. Для її уникнення за останніх часів було запропоновано використання упертих (*stubborn*) множин станів та скінчених префіксів розгортаних (*unfolding*) сітей [5-8].

Універсальна сіть Петрі [9] (УСП) виконує довільну задану сіть Петрі: на вхід УСП подають сіть Петрі та її початкове маркування; на виході отримують допустиме маркування та відповідну послідовність запуску переходів. Задана сіть Петрі, її маркування та послідовність запуску переходів зашифровано фіксованою кількістю цілих невід'ємних скалярних змінних, які подано як певні позиції УСП. Основу шифрування складає шифрування вектору цілих невід'ємних чисел як одного числа у позиційній системі числення, яке може бути виконане рекурентно функціями додавання до шифру *mul_add* та вилучення із шифру *mod_div*. Розроблено методику подання окремих операцій сітями Петрі та композиції алгоритмів через об'єднання позицій операторів та підстановку переходів підсітями, що реалізують операції, а також відповідну бібліотеку основних арифметичних та логічних операцій, правила копіювання вхідних та вихідних змінних операцій.

Для забезпечення сумісності із існуючими алгоритмічними системами на основі УСП побудовано сіті Петрі, що виконують довільну задану машину Тюрінга [10] й довільний заданий нормальний алгоритм Маркова [11]. В [10] розроблено методику роботи із стрічкою машини Тюрінга через два стека, що подають ліву та праву частини стрічки відносно до символу поточної комірки.

Отже створено теоретичні основи парадигми обчислень на сітях Петрі [12], що дозволяє подавати та виконувати довільні алгоритми та може бути застосованою для подання алгоритмів розгортання сітей Петрі, що й є *метою* даної роботи.

Аналіз наукових результатів із розгортання сітей Петрі

В. Котов [1] запропонував концепції сіті-системи та сіті-процесу. В основі концепції сіті-процесу лежить пропозиція застосування того ж самого формалізму сіті Петрі для подання динамічного процесу виконання довільної сіті Петрі (сіті-системи). В математиці та інформатиці в теоретичних дослідженнях ідея застосування тієї ж самої формальної системи для специфікації її поведінки або процесу виконання була в багатьох випадках достатньо продуктивною. Так, наприклад, А. Тюрінг застосував свою машину Тюрінга для виконання довільних машин Тюрінга та в результаті отримав концепцію універсальною машини, яка стала прототипом сучасних комп'ютерів й дозволила довести багато теоретичних результатів в теорії обчислень. Самозастосування машини Тюрінга дозволило зіткнутися із алгоритмічно нерозв'язними проблемами. Такий підхід є розповсюдженим також і в більш практичних галузях інформатики, наприклад, програмування компіляторів із певної алгоритмічної мови виконують на тій же самій мові, незважаючи на труднощі виконання першої компіляції самого компілятора.

Кен МакМіллан [5, 6] висунув приклад гри на дошці із певними обмеженнями на дозволені ходи, втіленням якої може бути імітація процесу запуску переходів сіті Петрі. Він визначив нескінченний процес розгортання сіті Петрі за допомогою п'яти правил виконання «ходів» у грі, заданій сіттю Петрі. Потім формально впровадив сіть реалізації подій (*occurrence net*), як подання процесу розгортання вихідної сіті Петрі.

Основною перешкодою в практичному застосуванні розгортаних сітей є той факт, що вони є нескінченими у загальному випадку. Для подолання цієї перешкоди МакМілан висунув концепцію усіченого (*truncated*) розгортання на основі понять локальної конфігурації та точки відсічення (*cutoff point*), що надало йому можливість доказати низку теорем про зв'язок властивостей вихідної сіті Петрі із виглядом усіченої розгортаної сіті.

В подальших роботах по розгортанню сітей Петрі [7, 8] скінчену усічену розгортану сіть було названо префіксом розгортання та було запропоновано декілька вдосконалень загального методу як із точки зору мінімальності префіксу, так із позицій ефективних методів пошуку властивостей, зокрема тупиків.

Найбільш досконалим вважається метод, запропонований Дж. Еспарзою у купі із співавторами [8], що дає найменший із відомих префіксів, придатних у застосуваннях аналізу властивостей. Для заданою сіті Петрі, по-перше, введено поняття позначеної сіті, у якої вершини позначено символами вершин вихідної сіті та відносно якої зберігається відношення послідовності маркувань при запуску переходу. У той же самий спосіб для довільного графу може бути отримано дерево реалізації подій, виходячи із певної множини умов; введено поняття процесу розгалуження (*branching process*) як сіті реалізації подій, отриманої за допомогою розгортання вихідної сіті.

Для подання сіті реалізації подій на множені вершин введено відносини причинності (*causal*), конфлікту (*conflict*) та конкуренції (*concurrency*). Позиції сіті реалізації подій мають не більше одного входу; сіть ациклічна, тобто причинне

відношення є відношенням часткового порядку; сіть скінчено випереджена; ніякий елемент не знаходиться у конфлікті із собою.

Процес розгалуження введено як сіть реалізації подій із додатковими обмеженнями на функцію позначання: зберігає природу вершин; зберігає оточення вершин; починається із начального маркування; не дублює переходи сіті. Приклад процесу розгалуження подано на рис. 1.

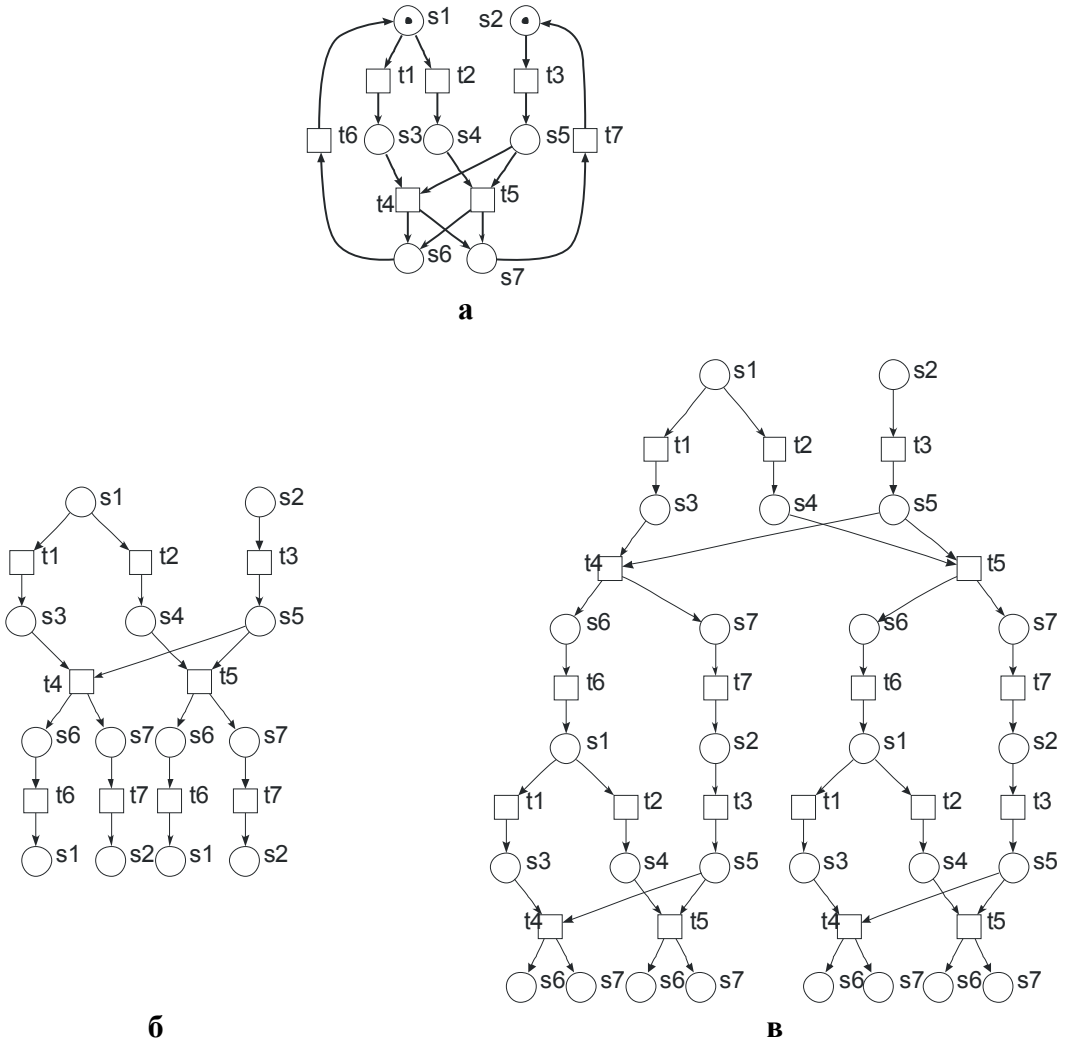


Рис. 1. Приклад процесу розгалуження [8]: а – вихідна сіть; б – три рівні розгортання; в – п’ять рівнів розгортання

Потім введено поняття префіксу процесу розгалуження через приналежність мінімальною частки, а також попередніх подій довільної умови і попередніх та наступних умов довільної події. Розглянуто процес розгортання за принципом «як можна більше» та встановлено зв’язок графів досяжних маркувань вихідної сіті та процесів розгалуження.

Для отримання оптимальних префіксів введено поняття *конфігурації та зрізу* процесу розгалуження. Процес розгалуження сіті Петрі $\sum = (S, T, W, M_0)$ подано як позначену сіть реалізації подій $\beta = (O, p) = (B, E, F, p)$ у вигляді множини вершин $\{n_1, ..., n_k\}$, де вершина – це умова або подія. Умову подано як пару (s, e), де s – позиція сіті $\sum$, e – покажчик вхідної події (можливо пустий *nil*). Подію подано як пару (t, X), де t перехід сіті $\sum$, X список покажчиків на вхідні умови. Нехай t – це перехід сіті $\sum$

із вихідними позиціями $s_1,...,s_n$. $PE(\beta)$ позначає *множину можливих розширень процесу розгалуження*: пара $e=(t,X)$ є можливим розширенням процесу розгалуження $\{n_1,...,n_k\}$, якщо множина $\{n_1,...,n_k,e,(s_1,e),...,(s_n,e)\}$ також є процесом розгалуження. Начальний процес *Unf* містить тільки умови, що відповідають начальному маркуванню M_0; якщо $M_0(s)=k$, процес містить k елементів (s,nil).

Алгоритм розгалуження за [8]:

```
pe:=PE(Unf);
while pe≠nil do
     додати до Unf подію e=(t,X) із pe та умову (s,e) для кожної
     вихідної позиції s переходу t;
     pe:=PE(Unf);
endwhile
```

Для процесів автоматизації виробництва [2, 3] найбільш важливими є такі властивості сітей Петрі [1-3], як обмеженість, консервативність, живість, досяжність вказаного маркування; критичним для втілення автоматизованого виробництва є існування тупиків, що зумовлює актуальність задачі примусової живості [4]. МакМілан [5, 6] отримав результати стосовно обмеженості сіті й досяжності та покривності певного маркування. Таубін, Кондратьєв та Кішинєвський [7] запропонували методи уникнення тупиків на основі розгортання та довели, що отримані «покращені» сіті мають менший розмір за відомі інші методи та працюють на більш загальному класі сітей. Дж. Есларза та ін. [8] отримали окремі результати стосовно ефективного аналізу властивостей підкласів *k*-обмежених сітей.

Побудова універсальної розгортаючої сіті Петрі

Універсальна розгортаюча сіть Петрі (УРСП), схему якої зображено на рис. 2, по заданій довільній ординарній сіті Петрі та її початковому маркуванню, що у купі позначено як $\Sigma=(S,T,W,M_0)$, будує процес розгалуження $\beta=(O,p)=(B,E,F,p)$ відповідно до позначень, що наведені вище. Якщо процес розгалуження нескінчений, УРСП будує його довільний скінчений префікс.

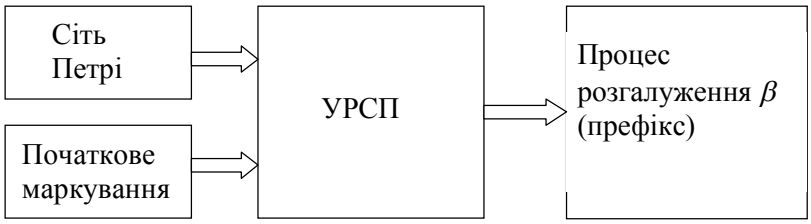


Рис. 2. Схема роботи УРСП

1) Шифрування сіті Петрі та процесу розгалуження.

Усі змінні УРСП мають бути подані як цілі невід'ємні числа – маркування певних позицій. У шифруванні векторів та матриць використано рекурсивні алгоритми та допоміжні сіті УСП [9]: *mul_add* – додавання до шифру, *mod_div* – вилучення із шифру. На відміну від УСП, для побудови УРСП використано вектори із змінною кількістю компонентів; дійсну кількість компонентів подано у перших елементах відповідного запису. Для шифрування компонентів обрана основа r, що перевищує значення m, n кількості позицій та переходів і дозволяє побудувати достатньо великий префікс. Число

r є обмеженням на кількість умов та подій префіксу. Використано фіксовану наперед задану основу; динамічне збільшення основи у процесі побудови префіксу є напрямом подальших робіт.

Основні дані алгоритму подано як масиви записів чотирьох різновидів (рис. 3): переходи rt та позиції rp для подання вихідної сіті Петрі, умови rc та події re для подання префіксу; значення змінних nin, $nout$ – кількість вхідних та вихідних вершин відповідно.

rt::

nin	nout	p[]	…

rp::

nout	t[]	…

rc::

p	nout	e[]	…

re::

t	nout	c[]	…

Рис. 3. Формати основних записів.

Для шифрування масивів записів обрано підхід стрічки із двома стеками для подання лівої та правої сторін стрічки [10] та поточного запису із окремим поданням поточного елементу масиву наступних вершин. Використані позиції, що відповідають шифрам масивів записів та елементам поточних записів, наведено на рис. 4.

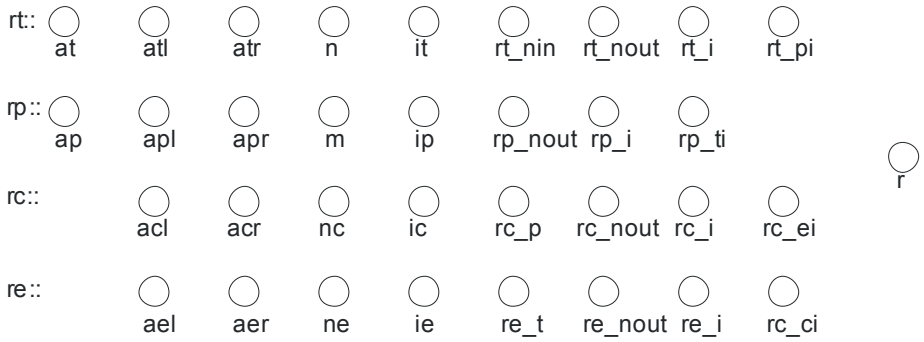


Рис. 4. Подання шифрів основних структур даних

Позиції at, ap, ac, ae подають шифри масивів переходів, позицій, умов та подій відповідно. Суфікси «l», «r» додаються для подання лівої та правої частини стрічки відповідно; окреме подання шифрів використано тільки для масивів переходів та позицій через те, що вони не змінюються в процесі побудови процесу розгалуження.

Позиції n, m, nc, ne визначають кількість переходів, позицій, умов та подій відповідно. Позиції it, ip, ic, ie визначають номер поточного переходу, позиції, умови та події відповідно; нумерацію виконано від одиниці, значення нуля має спеціальне використання.

Запис переходу має масив вхідних та вихідних позицій; запис позиції – тільки масив вихідних переходів; запис умови – тільки вихідні події; запис події – тільки вихідні умови. Префікси rt, rp, rc, re позначають запис переходу, позиції, умови та події відповідно. Суфікси мають наступне значення: $\_p$, $\_t$ – номери позиції та переходу відповідно; $\_nin$, $\_nout$ – кількість вхідних та вихідних вершин відповідно; $\_i$ –

індекс поточної вершини із масиву вхідних/вихідних вершин; $\_ti$, $\_pi$, $\_ci$, $\_ei$ – значення поточного елементу масиву вершини.

Доступ до елементів масивів вхідних/вихідних вершин організовано послідовно із поданням тільки поточного елементу та переміщенням вдовж відповідної стрічки вліво/вправо для доступу до попереднього/наступного елементу. Шифрування масивів переходів, позицій, умов та подій виконано від менших індексів для надання можливості дописування нових умов/подій у кінець. Для поточного запису, шифрування виконане у зворотному порядку від елементів масивів із старшими індексами, що забезпечує послідовний доступ у прямому порядку через використання функції *mod_div*. Для масивів умов та подій реалізовано збереження правої частини стрічки із використанням функції *mul_add*. Приклад порядку шифрування елементів масиву подій наведено на рис. 5.

c[*k1*]	…	*c*[*1*]	*re_nout*	*re_t*	…	*c*[*kne*]	…	*c*[*1*]	*re_nout*	*re_t*
Подія re[1]						Подія *re*[*ne*]				

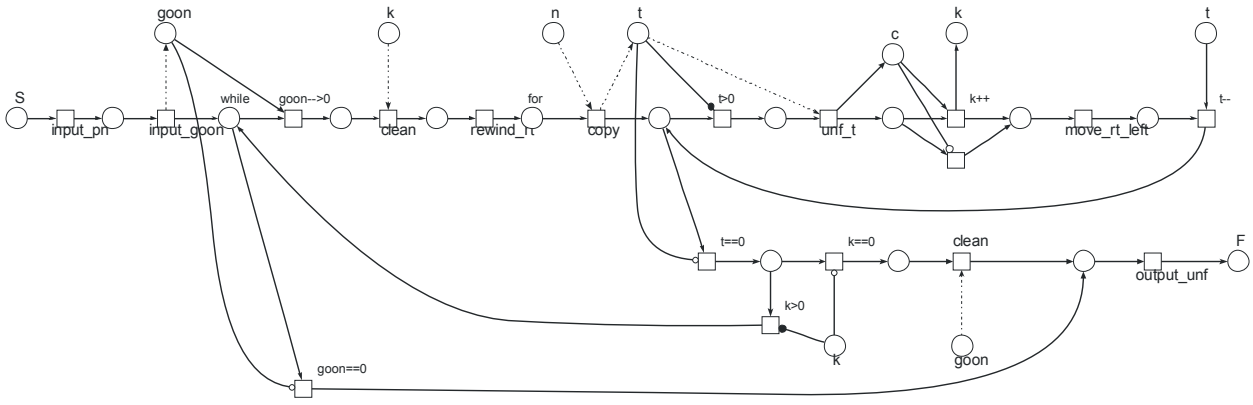
Рис. 5. Порядок шифрування масиву подій

Використаний наступний порядок доступу до зашифрованих стрічок: пересування по записах вліво реалізовано безпосередньо; пересування вправо – через перемотування стрічки до правого кінці та наступне пересування вліво. До зашифрованих масивів вхідних/вихідних вершин поточного запису реалізовано безпосереднє пересування в двох напрямках. Такий порядок зумовлений тим, що інформація про довжину масиву вершин поточного запису знаходиться з правого боку.

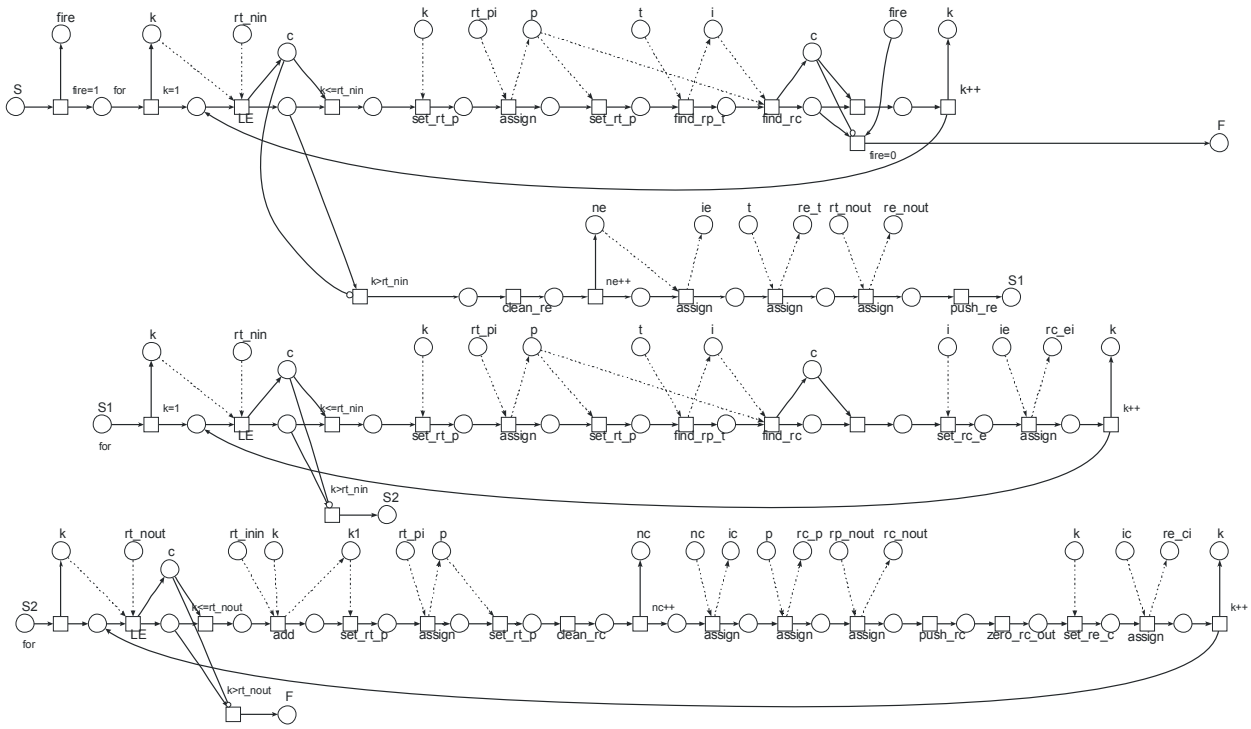
2) Основні компоненти універсальної розгортаючої сіті Петрі.

Універсальну розгортаючу сіть Петрі побудовано через деталізацію та кодування алгоритму Еспарзи [8], інгібіторною сіттю Петрі [9-11] відносно до шифрування використаних структур даних цілими невід'ємними числами. Отриману УРСП подано на рис. 6.

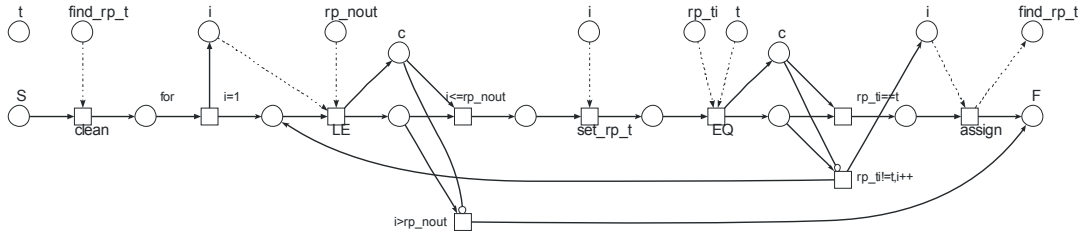
Основна сіть UUFPN виконує введення сіті Петрі та її шифрування із створенням масиву початкових умов через підсіть *input_pn* й введення кількості рівнів розгортаної сіті *input_goon*, послідовну побудову процесу розгалуження через викликання підсіті *unf_t*(*t*), що реалізує додавання події, відповідної до спрацьовування вказаного переходу *t*, а також виведення побудованої розгортаної сіті через підсіть *output_unf*. Підсіть *rewind_rt* виконує перемотування стрічки переходів вправо; підсіть *move_rt_left* – переміщення до наступного переходу зліва. На кожному рівні переходи перебираються послідовно; додатковою умовою завершення є відсутність активних переходів $!k$.



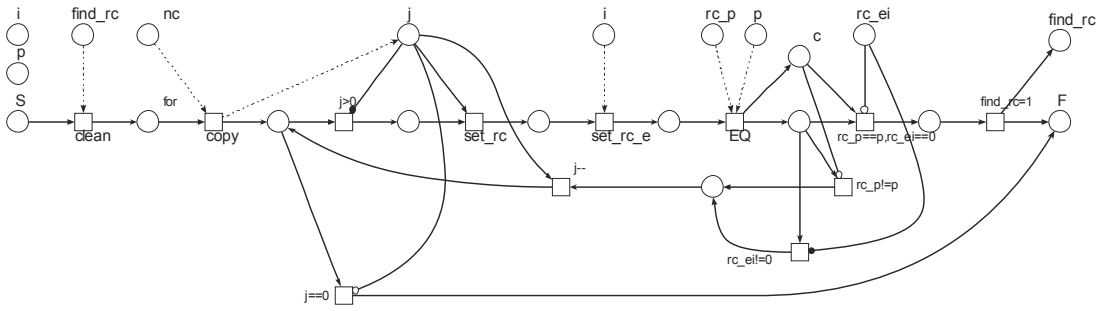
а



б



в



г

Рис. 6. Універсальна розгортаюча сіть Петрі: а – головна сіть UUFPN; б – підсіть розгортання переходу *unf_t*; в – підсіть пошуку індексу переходу для поточної позиції *find_rp_t*; г – підсіть пошуку події *find_rc*

Підсіть *unf_t* виконує додавання до процесу розгалуження події, що відповідає спрацьовуванню переходу *t* у тому разі, якщо присутні умови спрацьовування цього переходу; нова подія додається у купі із вихідними умовами, які створює означена подія.

Перший цикл по змінній *k* перевіряє наявність вхідних умов події – збудження переходу. Виклик підсіті *set_rt_p*(*k*) та присвоєння $p = rt\_pi$ обирають вхідну позицію переходу, на яку встановлюється відповідна стрічка через *set_rp*(*p*). Виклик функції

$i = find\_rp\_t(t)$ знаходить індекс i переходу t серед вихідних переходів позиції. Виклик функції $find\_rc(p,i)$ знаходить відповідну невикористану умову в розгортаній сіті, якщо вона присутня.

Якщо по завершенні циклу змінна *fire* залишається встановленою, перехід є збудженим, що викликає додавання відповідної події. Наступні два цикли по змінній *k* виконують обробку вхідних та вихідних умов доданої події відповідно та формування самого запису нової події.

Підсіть *clean_re* виконую перемотування стрічки подій в правий край; кількість подій збільшується $ne++$ та встановлюється індекс доданої події $ie = ne$. Встановлюється значенні відповідного переходу $re\_t = t$ та кількості його вихідних позицій (вихідних умов доданої події) $re\_nout = rt\_nout$; встановлені значення додаються до шифру підсіттю *pust_re*, яка встановлює індекс поточного елементу масиву вихідних умов події $re\_i = 1$.

Цикл по змінній *k* від одиниці до *rt_nin* встановлює ознаку використання вхідних умов доданої події. В процесі розгалуження умову може бути використано переходом із певним номером тільки один раз. Спочатку всі вихідні події умови встановлено рівними нулю; якщо умову використано переходом, то до запису умови додаються номер відповідної події в елемент, індекс якого відповідає переходу. Спочатку цикл дублює дії попереднього циклу, потім встановлює елемент умови через *set_rc_e*(*i*) та присвоює його значення $rc\_ei = ie$.

Цикл по змінній *k* від одиниці до *rt_nout* створює вихідні умови доданої події, що відповідають вихідним позиціям поточного переходу. Виклик підсіті $set\_rt\_p(rt\_nin + k)$ та присвоєння $p = rt\_pi$ обирають вихідну позицію переходу, на яку встановлюється відповідна стрічка через *set_rp*(*p*); параметр виклику підсіті *set_rt_p* має вигляд $rt\_nin + k$, що відповідає вихідній позиції із номером *k*, які розміщуються після вхідних позицій, кількість яких *rt_nin*. Підсіть *clean_rc* виконую перемотування стрічки умов в правий край; кількість умов збільшується $nc++$ та встановлюється індекс доданої умови $ic = nc$. Встановлюється значенні відповідної позиції $rc\_p = p$ та кількості її вихідних переходів (вихідних подій доданої умови) $rc\_nout = rp\_nout$; встановлені значення додаються до шифру підсіттю *push_rc*. Підсіть *zero_rc_out* занулює значення вихідних подій умови та додає їх до шифру стрічки умов. Тіло циклу завершується встановленням покажчика події на додану умову: виклик підсіті *set_re_c*(*k*) встановлює відповідну умову за вказаним індексом на стрічці подій, а потім виконується присвоєння номеру умови $rc\_ci = ic$.

Підсіть *unf_t* повертає значення *fire*, що дорівнює одиниці у разі збудження вказаного переходу та додавання відповідної події до процесу розгалуження, в іншому разі повертається нульове значення.

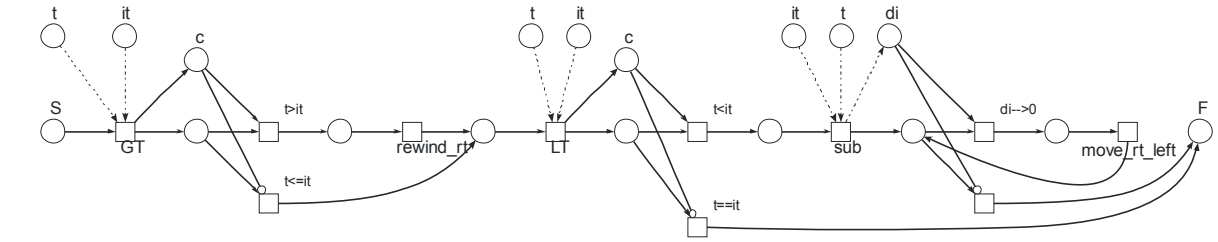
Допоміжна підсіть *find_rp_t* знаходить індекс переходу із вказаним номером *t* в масиві вихідних переходів поточної позиції; у випадку використання коректних даних результат пошуку завжди позитивний. Підсіть *find_rc* є основною у формуванні нових подій; за номером позиції *p* та індексом *i* поточного переходу у масиві вихідних переходів позиції підсіть *find_rc* знаходить відповідну умову, яку можна використати для створення події. Цикл по *j* від *nc* до 1 задає перевірку всіх умов; виклик підсіті *set_rc*(*j*) встановлює поточну умову, виклик підсіті *set_rc_e*(*i*) встановлює вихідну подію умови із індексом *i*. Перевірка $rc\_p == p$ визначає, що умова відповідає позиції *p*, а перевірка $rc\_ei == 0$ визначає, що умова не використана переходом із індексом *i*.

3) Підсіті роботи із шифрами структур даних.

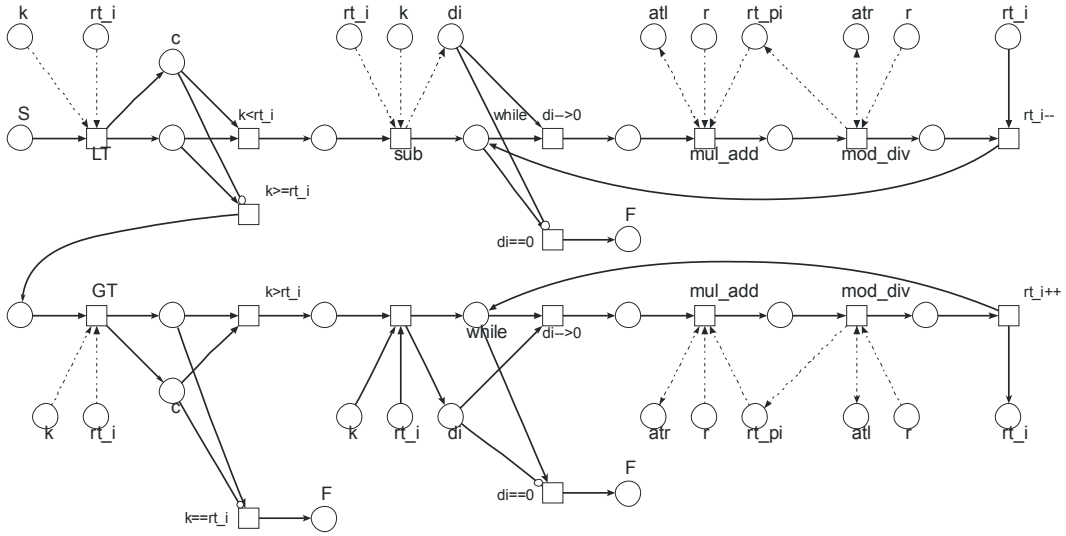
Робота із шифрами структур даних, описаних в попередніх розділах, вимагає додаткових процедур забезпечення доступу до зашифрованих елементів. Зауважимо, що алгоритм використовує певну кількість цілих невід'ємних змінних, які подані

відповідними позиціями сіті Петрі (рис. 4). Допоміжні підсіті доступу до шифрів наведено на рис. 7.

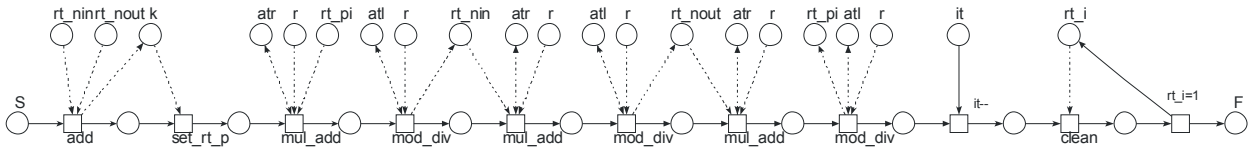
Повний набір містить підсіті, що відповідають переходам (t), позиціям (p), умовам (c), подіям (e) та примітивам шифрування (*encoding*); на рис. 7 наведено основні підсіті. Масив записів кожного різновиду подано як стрічку цілих чисел [10], послідовний доступ до елементів якої виконується за допомогою двох стеків шифрів лівої (l) та правої (r) частин й поточного елементу із внутрішнього масиву змінної довжини поточного запису.



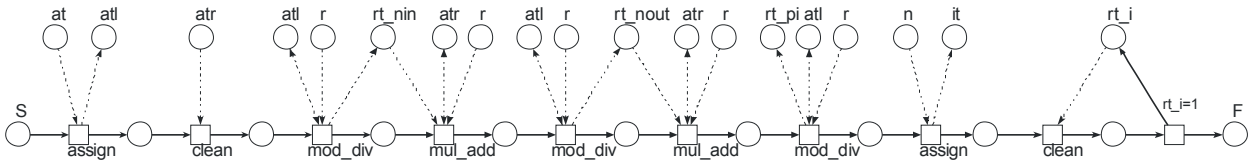
а



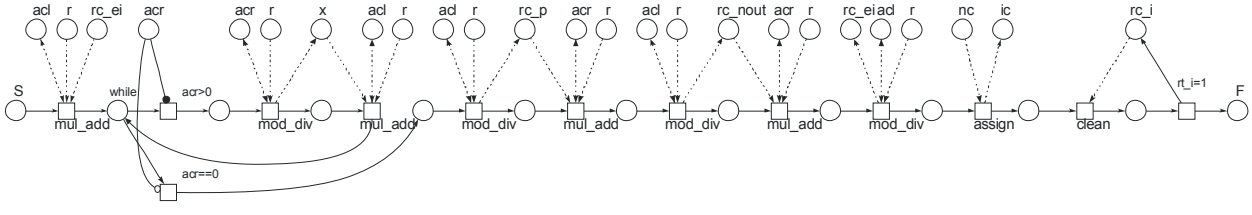
б



в



г



д

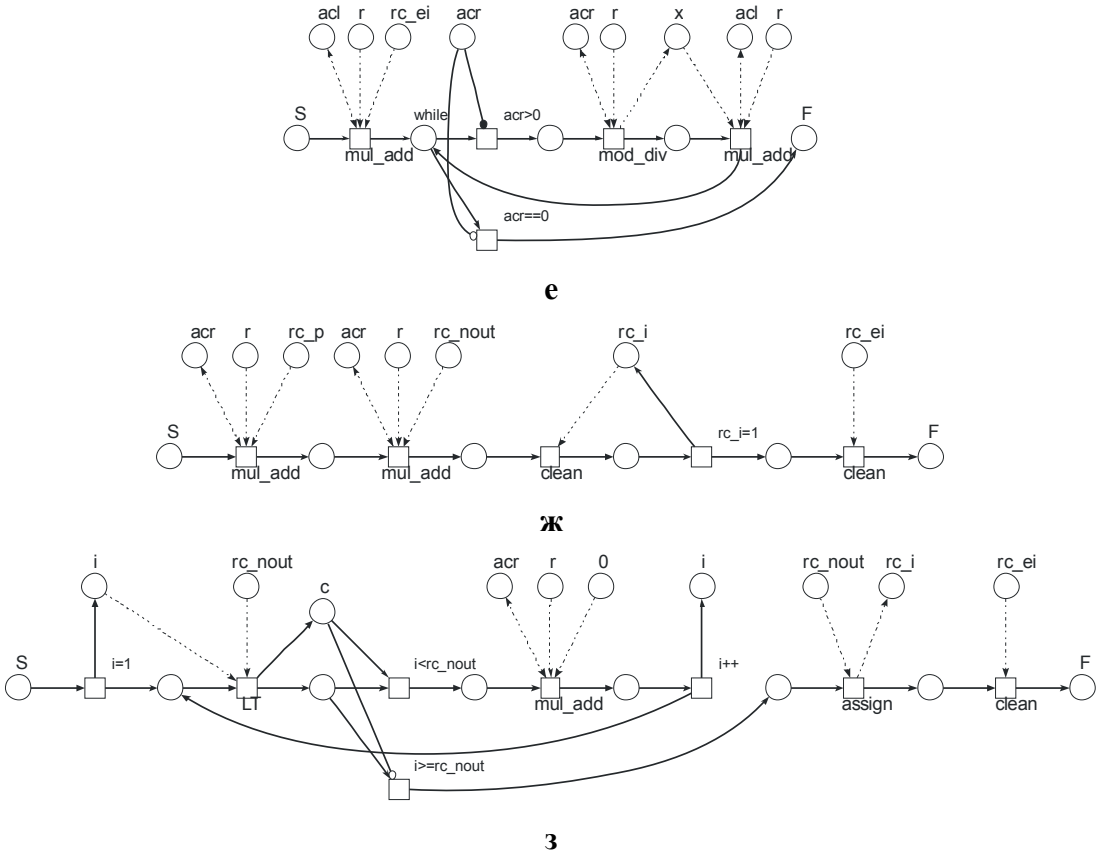


Рис. 7. Підсіті доступу до шифрів структур даних: а – підсіть встановлення запису вказаного переходу *set_rt*(*t*); б – підсіть встановлення вхідної/вихідної позиції поточного переходу *set_rt_p*(*k*); в – підсіть переміщення на один запис переходу вліво *move_rt_left*; г – підсіть перемотування стрічки переходів вправо *rewind_rt*; д – підсіть перемотування стрічки умов вправо *rewind_rc*; е – підсіть перемотування стрічки умов вправо для додавання нової умови *clean_rc*; ж – підсіть збереження префіксу нової умови *push_rc*; з – підсіть занулення вихідних подій нової умови *zero_rc_out*

Суттєво відрізняються підсіті роботи із масивами, які не змінюються у процесі роботи – переходи та позиції вихідної сіті Петрі, та масивами, які створюються у процесі виконання УРСП – умови та події процесу розгалуження.

Підсіть *set_rt* (рис. 7(а)) встановлює вказаний поточний запис стрічки переходів; підсіть *set_rt_p* (рис. 7(б)) встановлює вказаний поточний елемент масиву вхідних/вихідних позицій поточного переходу; підсіть *move_rt_left* (рис. 7(в)) переміщує стрічку на один запис вліво; підсіть *rewind_rt* (рис. 7(г)) перемотує стрічку вправо до кінця. Аналогічні підсіті створено для стрічок позицій та умов. Для стрічки подій виконується доступ тільки до останнього запису, що є крайнім з правої сторони стрічки; тому присутня тільки підсіть *set_re_c* встановлення поточної умови із масиву вихідних умов події.

Перемотування стрічок переходів та позицій реалізовано простим присвоєння, наприклад, *rewind_rt* (рис. 7(г)) для стрічки переходів: $atl = at$; $atr = 0$. Перемотування стрічки умов *rewind_rc* (рис. 7(д)) реалізовано по елементах із збереженням лівої частини стрічки

```
mod_div(&x, &acr, r)
mul_add(&acl, r, x)
```

Після переміщення на запис вліво або перемотування виконується обробка префіксу поточного запису та встановлення на перший елемент внутрішнього масиву. Обробка префіксу супроводжується його збереженням через стандартну послідовність примітивів шифрування, наприклад, в процедурі *move_rt_left*:

```
mod_div(&rt_nout, &atl, r)
mul_add(&atr, r, rt_nout)
```

Перша процедура *mod_div* витягає значення *rt_nout* із лівої частини стрічки *atl*, а потім процедура *mul_add* додає витягнуте значення до правої частини стрічки *atr*.

Виключенням є робота із шифрами внутрішніх масивів (подій для $rc\_$), де переміщення відбувається із запізненням. Витягнутий елемент зберігається у змінній *rc_ei* (його індекс визначає *rc_i*) та додається до шифру при наступному переміщенні

```
mul_add(&acl, r, rc_ei)
mod_div(&rc_ei, &acr, r)
```

Таким чином реалізовано можливість модифікації внутрішніх записів масиву умов для посилання на створену подію.

При створенні нових умов та подій передбачено їхнє додавання у правий край стрічки. Наприклад, для умов процедура *clean_rc* (рис. 7(е)) перемотує у правий край повністю (без встановлення на останній запис). Після присвоєння значень змінним префіксу *rc_p*, *rc_nout* поточного запису визивається процедура *push_rc* (рис. 7(ж)), яка додає їх до правої частини стрічки та надає можливість роботи із масивом вихідних подій, який занулюється процедурою *zero_rc_out* (рис. 7(з)) із збереженням шифру у правій частині стрічки.

Переміщення по внутрішніх масивах записів процедурами *set_rt_p*, *set_rp_t*, *set_rc_e*, *set_re_c* виконується залежно від оцінки напрямку, що визначається значенням поточного індексу та параметру *k*. Наприклад, для *set_rt_p* (рис. 7(а)): у разі $k < rt\_i$ переміщення вправо, у разі $k > rt\_i$ переміщення вліво, інакше переміщення не потрібне. Змінна *di* дорівнює кількості елементів для переміщення, наприклад, $di = rt\_i - k$ для переміщення вправо. Потім у циклі виконується переміщення по елементах

```
while(di-- > 0)
{
     mul_add(&atl, r, rt_pi);
     mod_div(&rt_pi, &atr, r);
     rt_i--;
}
```

Поточний елемент *rt_pi* долучається до шифру лівої частини стрічки *atl* процедурою *mul_add*, значення нового поточного елементу *rt_pi* вилучається із правої частини стрічки *atr* процедурою *mod_div* із зменшенням значення індексу rt_i--. Переміщення вліво вимагає зворотного використання частин стрічки *atr* у *mul_add* та *atl* у *mod_div* із збільшенням значення індексу rt_i++.

Переміщення по записах *set_rt*, *set_rp*, *set_rc* виконується за допомогою послідовного переміщення на один запис вліво *move_rt_left*, *move_rp_left*, *move_rc_left* відповідно у випадку переміщення вліво; переміщення вправо реалізовано через повне перемотування стрічки вправо на останній запис процедурами *rewind_rt*, *rewind_rp*, *rewind_rc* відповідно та наступним переміщенням вліво.

Як наслідок способу побудови сіті UUFPN та її компонентів через кодування відомого алгоритму процесу розгалуження [8] за раніше перевіреною методикою [9-11] випливає наступне твердження.

Твердження. Сіть UUFPN є універсальною розгортаючою сіттю Петрі.

Висновки

Виконано огляд методів розгортання сітей Петрі та їх використання для дослідження властивостей, зокрема, пошуку тупиків та примушення живості. Виконано огляд теоретичних основ парадигми обчислень на сітях Петрі, яку обрано для побудови універсальної розгортаючої сіті Петрі. Розроблено методику шифрування сіті Петрі та префіксу розгалуження певною кількістю цілих невід'ємних змінних та підсіті доступу до шифрів. Розроблено універсальну розгортаючу сіть Петрі, яка використовує позиції, що містять шифр вихідної сіті Петрі та побудованого префіксу процесу розгалуження.

Напрямками подальших робіт є побудова мінімального префіксу процесу розгалуження та компонентів із дослідження властивостей заданої сіті Петрі безпосередньо у процесі роботи УРСП.

Список літератури

1. Котов В.Е. Сети Петри [Текст] / В.Е. Котов. – М. : Наука, 1984. – 160 с.
2. Слепцов А.И. Автоматизация проектирования управляющих систем гибких автоматизированных производств [Текст] / А.И. Слепцов, А.А. Юрасов ; под ред. Б.Н. Малиновского. – К. : Техніка, 1986. – 158 с.
3. Li Z.W. Deadlock Resolution in Automated Manufacturing Systems: A Novel Petri Net Approach / Z.W. Li, M.C. Zhou. – New York: Springer-Verlag, 2009. – 239 p.
4. Liu D. Liveness of an Extended S^3PR / D. Liu, Z.W. Li, and M.C. Zhou // Automatica. – 2010. – Vol.46, Iss.6. – PP. 1008-1118.
5. McMillan K.L. Using unfoldings to avoid the state explosion problem in the verification of asynchronous circuits // Computer Aided Verification, Fourth International Workshop, CAV '92, Montreal, Canada, June 29 - July 1, 1992, Proceedings. Lecture Notes in Computer Science. – 1993. – Vol.663. – PP. 164-174.
6. McMillan K.L. A Technique of State Space Search Based on Unfolding / K.L. McMillan // Formal Methods in System Design. – 1995. – Vol.6, No.1. – PP. 45-65.
7. Taubin A. Deadlock Prevention Using Petri Nets and their Unfoldings / A. Taubin, A. Kondratyev, and M. Kishinevsky // International Journal of Advanced Manufacturing Technology. – 1998. – Vol.14, No.10. – PP. 750-759.
8. Esparza J. An Improvement of McMillan's Unfolding Algorithm / J. Esparza, S. Römer, W. Vogler // Formal Methods in System Design. – 2002. – Vol.20, No.3. – PP. 285-310.
9. Зайцев Д.А. Універсальна мережа Петрі / Д.А. Зайцев // Кибернетика и системный анализ. – 2012. – № 4. – С. 24-39.
10. Зайцев Д.А. Ингибиторная сеть Петри, исполняющая произвольную заданную машину Тьюринга / Д.А. Зайцев // Системні дослідження та інформаційні технології. – 2012. – № 2. – С. 26–41.
11. Зайцев Д.А. Ингибиторная сеть Петри, выполняющая произвольный заданный нормальный алгорифм Маркова // Моделирование и анализ информационных систем. – 2011. – Том 18, №4. – С. 80-93.
12. Zaitsev D.A. Petri Net Paradigm of Computation // Proceedings of the International scientific conference on Computer Algebra and Information Technology, August 20-26, 2012. – Odessa, 2012. – PP. 107-114.

УНИВЕРСАЛЬНАЯ РАЗВОРАЧИВАЮЩАЯ СЕТЬ ПЕТРИ

Д.А. Зайцев[1], Жи Ву Ли[2], Лианг Хонг[2]

[1] Международный гуманитарный университет,
Фонтанская дор., 33, Одесса, 65009, Украина; e-mail: zsoftua@yahoo.com
[2] School of Electro-Mechanical Engineering, Xidian University,
2 South TaiBai Road, Xi'an, 710071, China; e-mail: systemscontrol@gmail.com

Разработана универсальная разворачивающая сеть Петри, которая по произвольной заданной ординарной сети Петри строит конечный префикс процесса ветвления. Разработано шифрование сети Петри и процесса ветвления определенным количеством целых неотрицательных чисел, которые представлены как позиции универсальной разворачивающей сети Петри, и набор подсетей для работы с шифрами. Использованы основы парадигмы вычислений на сетях Петри по программированию на языке ингибиторных сетей Петри посредством композиции подсетей, которые представляют основные операции и операторы.
Ключевые слова: разворачивание сетей Петри, процесс ветвления, живость, универсальная сеть Петри, парадигма вычислений на сетях Петри

UNIVERSAL UNFOLDING PETRI NET

Dmytro A. Zaitsev[1], Zhi Wu Li[2], Liang Hong[2]

[1] International Humanitarian University,
33 Fontanskaya Road, Odesa, 65009, Ukraine; e-mail: zsoftua@yahoo.com
[2] School of Electro-Mechanical Engineering, Xidian University,
2 South TaiBai Road, Xi'an, 710071, China; e-mail: systemscontrol@gmail.com

Universal unfolding Petri net was developed that builds a finite prefix of the branching process on arbitrary given ordinary Petri net. An encoding of Petri net and the branching process by a certain number of nonnegative integer numbers which are represented as places of universal unfolding net and a series of subnets for the codes processing were developed. The foundations of Petri net paradigm of computation are employed regarding the programming in the language of inhibitor Petri nets via composition of subnets which represent basic operations and operators.
Keywords: Petri net unfolding, branching process, liveness, universal Petri net, Petri net paradigm of computation

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

Том 2, номер 2, 2012. Одеса – 99 с., іл.

ИНФОРМАТИКА И МАТЕМАТИЧЕСКИЕ МЕТОДЫ В МОДЕЛИРОВАНИИ

Том 2, номер 2, 2012. Одесса – 99 с., ил.

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Volume 2, No. 2, 2012. Odesa – 99 p.

Засновник: Одеський національний політехнічний університет

Зареєстровано Міністерством юстиції України 04.04.2011р.

Свідоцтво: серія КВ № 17610 - 6460Р

Друкується за рішенням Вченої ради Одеського національного політехнічного університету (протокол №8 від 26.04.2011)

Адреса редакції: Одеський національний політехнічний університет,

проспект Шевченка, 1, Одеса, 65044 Україна

Web: http://www.immm.opu.ua

E-mail: immm.ukraine@gmail.com