МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний технічний університет України

“Київський політехнічний інститут імені Ігоря Сікорського”

Матеріали наукової конференції студентів, магістрантів та аспірантів

«Інформатика та обчислювальна техніка – ІОТ-2017»

23 травня 2017 року

(кафедра «Обчислювальної техніки»)

ТЕЗИ

Київ 2017

Оргкомітет конференції:

Голова:

О.А. Павлов – декан факультету, д.т.н., професор.

Заступник голови :

О .М. Долголенко – заст. декана по науковій роботі, к.т.н., доцент

Співголови організаційного комітету:

С.Г. Стіренко – завідувач кафедрою ОТ, д.т.н., професор

Члени організаційного комітету:

Ю.О. Кулаков- д.т.н., професор кафедри ОТ

В.І. Жабін – д.т.н., професор кафедри ОТ

В.П. Симоненко - д.т.н., професор кафедри ОТ

Г.М. Луцький – д.т .н., професор кафедри ОТ

О.П. Марковський – к.т.н., доцент кафедри ОТ

Секретар конференції:

Н.Є. Куц Пров. інженер кафедри ОТ

ЗМІСТ

УДК 683.519

ВЕЦКО В.І.

ПРОГНОЗУВАННЯ СТАНУ БАТАРЕЇ ЕЛЕКТРИЧНИХ ТРАНСПОРТНИХ ЗАСОБІВ ДЛЯ ОЦІНКИ ЖИТТЄЗДАТНОСТІ ПРИ КАРШЕРІНГУ

Каршерінг компанії впроваджують електричні транспортні засоби (EVs) в свій автопарк. Однак дані свідчать про те, що в даний момент при використанні електромобілів, не вдається досягти задовільної комерції. Потенційною причиною цього є більш нагружене використання транспортного засобу, що характерне для короткочасної оренди автомобілів, а також наслідки нагруженого використання транспортного засобу для стану батареї (SoH). У цій статті здійснено прогнозування SoH двох однакових електромобілів, що використовуються в різних практиках автомобільного обміну. Для цього використовуються отримані дані, що від зарядних станцій і різних датчиків EV. Розуміння користувачами правил водіння та поведінки зарядки батареї може служити цінним орієнтиром для системи короткочасної оренди автомобілів. Зокрема, результати прогнозування показують, що в залежності від умов експлуатації, момент досягнення батареєю електромобіля свого теоретичного кінця життя може відрізнятися на чверть часу.

Car-sharing companies are introducing electric vehicles into their fleet. At this point shared electric vehicles systems are failing to reach satisfactory commercial viability. A potential reason for this is the effect of higher vehicle usage, which is characteristic of car sharing, and the implications on the battery's state of health (SoH). In this paper, we forecast the SoH of two identical EVs being used in different car-sharing practices. For this purpose, we use real life transaction data from charging stations and different electric vehicles sensors. The results indicate that insight into users' driving and charging behavior can provide a valuable point of reference for car-sharing system designers. In particular, the forecasting results show that the moment when the battery of an electric vehicle reaches its theoretical end of life can differ in as much as a quarter of the time when vehicles are shared under different conditions.

Ключові слова: ПРОГНОЗУВАННЯ СТАНУ; ОРЕНДА АВТОМОБІЛІВ; ЕЛЕКТРИЧНИЙ ТРАНСПОРТНИЙ ЗАСІБ (EV); ВОДІННЯ І ПОВЕДІНКА ЗАРЯДКИ; СТАН ЗДОРОВ'Я БАТАРЕЇ (SoH); ДЕГРАДАЦІЯ БАТАРЕЇ; СПІЛЬНА ЕКОНОМІКА

1. Вступ

В останні роки відбулося переосмислення особистої мобільності. Є дві основні мотивації для цього. По-перше, після десятиліть використання автомобілів, ми досягли точки, де транспорт відповідає за 23% світових викидів. Очевидно, що теперішня система мобільності є нестійкою в її нинішньому вигляді і що необхідні нові, більш стійкі та енергоефективні рішення. По-друге, дослідження показали, що особисті транспортні засоби використовуються в середньому близько години в день [1,2]. Припарковані більшу частину часу, вони займають цінний простір для суспільства. Цей ефект особливо помітний в міських районах, де населення продовжує зростати. За даними Всесвітньої організації охорони здоров'я, 54% від загального світового населення проживає в міських районах. Тільки в Європі, в міських районах проживає понад дві третини населення Європейського Союзу.

Одним з рішень є спільне використання автомобілів. Оренда автомобілів дозволить задовольнити потребу в особистій мобільності, при цьому забезпечуючи більш низькі витрати для фізичних осіб і більш високу зручність використання транспортних засобів, що робить автомобілі більш економічно ефективним [3]. Fellows і Pitfield аналізуючи витрати і вигоди для оцінки оренди автомобіля виявили, що люди отримують економічну вигоду за рахунок скорочення подорожей

за ціною до 50%, а економіка в цілому виграє за рахунок зменшення пробігу транспортних засобів, збільшення середньої швидкості та економії в паливі, зменшення аварій та викидів. Більш систематичні результати в географічно більшому масштабі можна знайти в дослідженні Шахін і Коена [2], які визначили, що кожен автомобіль спільного користування зменшує потребу на 4-10 приватних транспортних засобів у Європі, 6-23 в Північній Америці, і 7-10 в Австралії.

В цій статті порівнюється вплив двох різних практик використання автомобілів спільного користування на продуктивності батареї. Це робиться за рахунок докладних даних електрокарів і даних про підзарядку для прогнозування SoH батарей двох однакових електромобілів в різних практиках. Основні дослідницькі матеріали роботи можуть бути розташовані в наступних областях: (1) детальний аналіз спільного водіння користувачів електрокарів і частоти підзарядок, сподіваючись таким чином забезпечити додакову інформацію для планування транспортної системи; (2) вплив двох різних методів обміну електрокарів на SoH батареї, оцінити життєздатність цих методів.

2. Практики каршерінгу та їх користувачів

Ми порівнюємо два однакових електромобілі, що орендуються за двох різних практик каршерінгу. Перший автомобіль є васністю компанії, що здає в оренду більш ніж 800 електричних і звичайних транспортних засобів. Дані автомобілі доступні для оренди більш ніж 24000 користувачів. Правилами користування прописано, що після використання користувач зобов'язаний підключити автомобіль для підзарядки, що гарантує максимально заряджений акумулятор для наступного користувача. В системі бронювання користувачі вказують приблизно скільки кілометрів і часу триватиме їхня оренда, для спрощення планування обслуговування. Другий автомобіль знаходиться в спільній власності житлового комплексу, де жильці займаються доглядом спільного майна. Підхід заснований на понятті спільної економіки. Автомобіль активно експлуатується серед 35 членів. Система бронювання передбачає вказування часових інтервалів, протягом якого буде експлуатуватися автомобіль. Підзарядка транспортного засобу здійснюється тільки з ініціативи користувача. В обох випадках автомобіль повинен бути повернутий в початковий пункт. Обидва автомобілі експлуатуються в однакових кліматичних умовах та регіоні.

3. Розуміння споживачів – манера водіння та повернення

Для того, щоб забезпечити якомога повне розуміння того, як були використані електромобілі, детально досліджувалися манера водіння і зарядка обох груп користувачів. Дані зарядки було зібрано від зарядних станцій. Дані водіння було зібрано з транспортних засобів за допомогою GPS та CAN шини (швидкість автомобіля, струм, напруги, часові мітки, заряд, стан двигуна).

З огляду на використання загальних електромобілів, автомобілів членів однієї компанії, їх використовують в основному в якості другого автомобіля, з високою частотою в другій половині дня і у вихідні дні (22% поїздок всіх водіїв були зроблені у суботу). Члени спільного житла були більш схильні використовувати загальний EV в ранкові години (рис. 1).

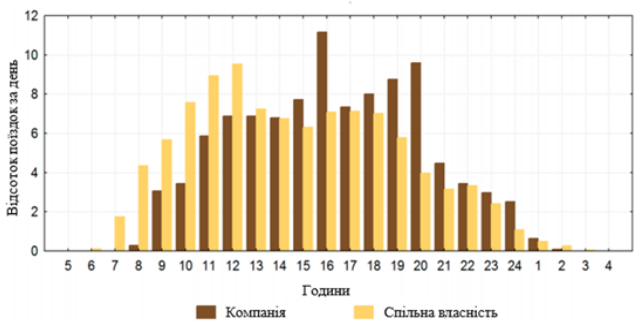

Рис. 1. Поведінка водіння, розподіл щоденних поїздок

При розгляді питання про тривалість зроблених поїздок, 72% поїздок користувачів спільно для будинку були коротше, ніж в 10 км. Згідно з офіційною статистикою стверджує, що середня поїздка автомобіля у Фландрії становить приблизно 34,4 км; середня поїздка

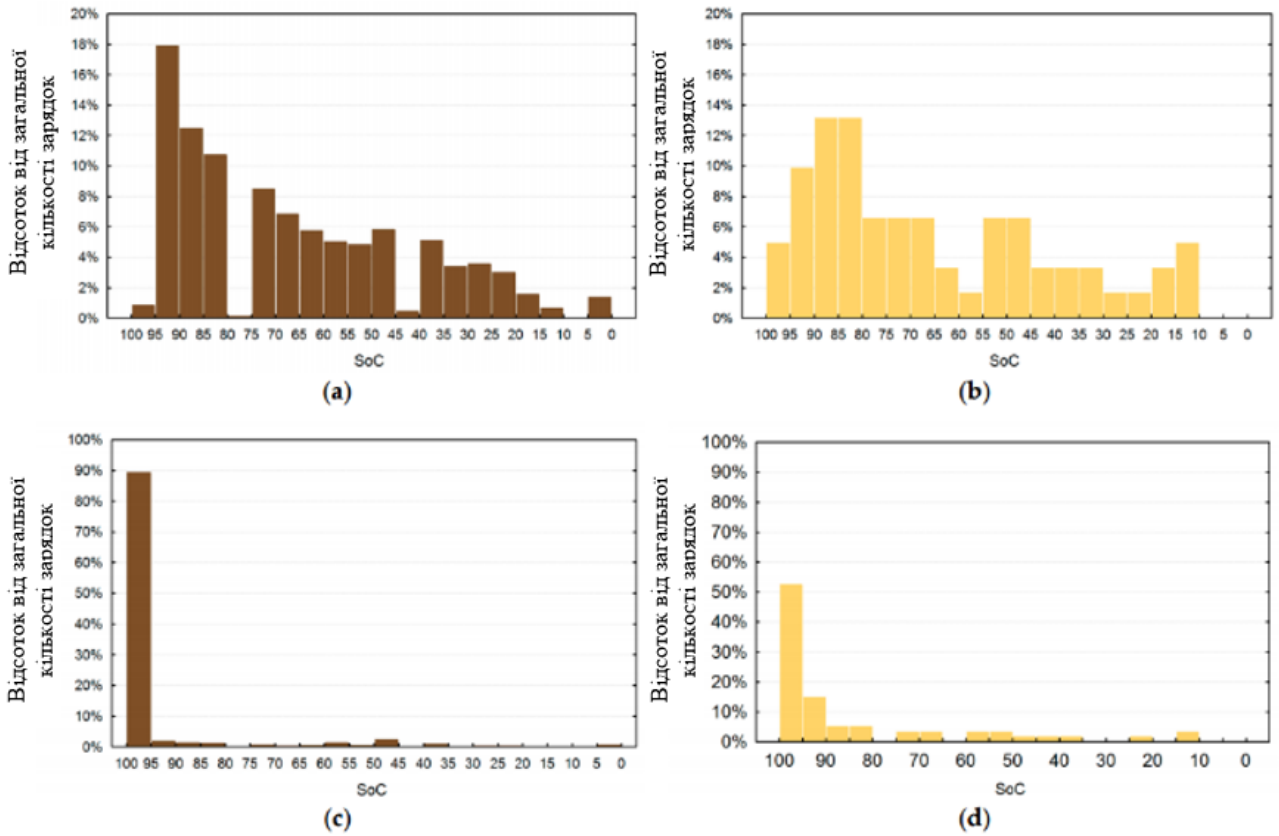

Рис. 2. Поведінки зарядки - стан заряду (SoC) на початку і в кінці зарядки; (a,c) SoC на початку та кінці зарядки для каршерінг компанії; (b,d) SoC на початку та кінці зарядки для автомобіля в спільній власності.

зроблені електромобілі належать автомобіля обміну компанії було 32,56 км, а шляхом спільного житла, 8,4 км.

З огляду на перезарядку, члени спільного житла, як правило, підзаряджали автомобіль зранку або пізно ввечері. Автомобіль каршерінгової компанії підключався після кожного використання. Таким чином автомобіль не буде від'єднано від зарядного пристрою до наступного користування, що іноді може зайняти більше тижня. В цілому, 7,6% підзарядок були зроблені з super charge. Всі перезарядки членами спільного житло були коротше, ніж день, де 33% з них були мене півгодини, і 4% з super charge.

Правила оренди також впливають на кількість зарядок в день. Для автомобілів каршерінгової компанії, число перезарядок переважно відповідає кількості користувачів в день (переважно один). Для спільного користування, транспортний засіб часто заряджається більше, ніж один раз в день. Беручи до уваги SoC батареї, то в 20% випадках автомобілі компанії заряджалися, але SoC батареї було вище, ніж 90%. У більшості випадків, батарея залишалася до повної зарядки. Для членів спільного користування, батарея повністю заряджалася тільки в половині випадків, в той час як значення SoC, при якому акумулятор був підключений на підзарядку, був більш рівномірно розподілений (рис. 2).

4. Методологія

Для того, щоб оцінити вплив практики каршерінгу, поведінку водіння та зарядки батареї електрокару, досліджувалися SoH, що визначаються як різниця між корисною місткістю і кінцевою місткістю [6]. SoH зазвичай виражається у вигляді відсотка від номінальної потужності і є мірою довгостроковості батареї [4,5]. У порівнянні з SoH, SoC визначається як відсоток від доступної ємності і є мірою короткочасної здатності батареї. Більш детально, SoC показує залишковий заряд батареї в даний момент, в порівнянні з енергією при повному заряді, що дає уявлення про те, скільки батарея працюватиме до наступної перезарядки. В аналогії зі звичайними автомобілями, SoC відповідає паливному манометру, в той час як SoH буде відповідає здатності

паливного бака зберігати паливо. У цій аналогії, паливний бак матиме змінний доступний обсяг.

У даній роботі SoH розраховується з даних експлуатації, в той час як SoC зібрана з CAN шини. Дані з CAN шини засобів зібрані з частотою 10 Гц. На рис. 3. показано миттєва передача потужності батареї (W) з плином часу під час експлуатації.

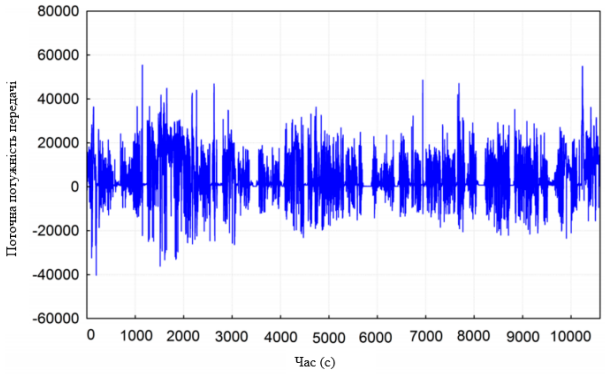

*Рис. 3. Графік V*I(W)*

На основі миттєвої передачі потужності батареї сумарна чиста енергія подається від акумуляторної батареї може бути обчислена шляхом трапецієподібної чисельного інтегрування струму батареї (I) і напруги (V) з плином часу, як показано рівнянням:

$$E_{te} = \int V * I \, dt$$

Крім того, знаючи SoC, на початку (SoC_1) і в кінці (SoC_2), SoH може бути визначений на основі рівняння:

$$SoH = \frac{E_{te}}{SoH_{100\%} * (SoC_1 - SoC_2)}$$

5. Вплив каршерінгу на стан батареї

Для обох електромобілів, використовуючи обчислення SoH з секції методології, ми визначили значення SoH для кожного циклу розрядки. Кількість записаних циклів трохи розрізнялися, для транспортного засобу, що належить компанії, було 59 і для автомобілю, що є спільній власності – 63. У літературі вказується, що протягом перших 500 циклів або близько того, ємність змінюється лінійно, обчислені значення SOH були використані для визначення цього лінійного тренда.

Для оцінки лінійного тренда і його застосовності для прогнозування майбутніх SoH елементів живлення, ми розрахували найменше квадратичне відхилення, середнє відхилення, відносну квадратичну похибку та відносне абсолютне відхилення:

$$LSD = \frac{\sum_{i=1}^{N}(E_i - O_i)^2}{N-1}$$

$$AD = \frac{\sum_{i=1}^{N}|E_i - O_i|}{N-1}$$

$$RSE = \frac{\sum_{i=1}^{N}[(E_i - O_i)/E_i]^2}{N-1}$$

$$RAD = \frac{\sum_{i=1}^{N}|E_i - O_i|/E_i}{N-1}$$

де: N – число спостережень або сума ваг; E_i – передбачене значення випадку і.

Таблиця 1 містить більш детальний аналіз оцінки лінійного тренда для обох автомобілів.

Табл. 1. Достовірність лінійних оцінок

Достовірність виміру	Спільна власність	Каршерінг компанія
LSD	1.605182	1.699434
AD	0.949703	1.07033
RSE	0.000184	0.00030
RAD	0.010116	0.01410

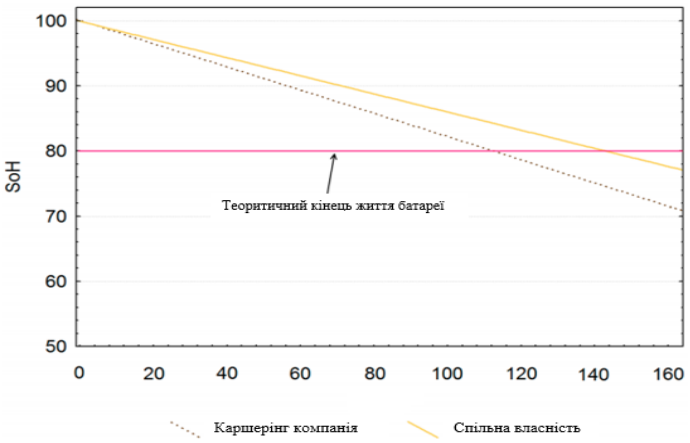

Рис. 4. Лінійна екстраполяція SoC тенденції і теоретичного кінця життя батареї

Як правило, це прийнято в автомобільній промисловості, час життя батареї вимірюється кількістю повних циклів її заряду-розряду (розряд батарея наступає, коли її номінальна потужності падає нижче 80% від її первісної номінальної потужності [7]). Екстраполяція лінійних трендів для EV батареї, показана на рис. 4.

7. Висновки

Дані від зарядних станцій і датчиків електрокарів можуть бути успішно використані для прогнозування SoH батареї. В статті збагачені існуючі імітаційні моделі в області оцінки SoH з емпіричним підтвердженням аналізу. Аналіз оснований на даних з двох однакових електромобілів, використання яких відрізнялося в середньому SoC, DoD і відсотком використання super charge. Результати вказують на те, що відстрочення зарядки і менше використання supper charge можуть уповільнити процес деградації батареї.

Крім того, деградація батареї пов'язана з вартістю батареї і вартістю автомобіля (вартість батареї складає близько 54% від загальної вартості автомобіля [8]). Дані висновки можуть бути цінним довідником для каршерінгу електрокарів і можуть бути інтегровані в існуючі системи каршерінгу.

Список літератури

1. Meijkamp, R. Changing consumer behaviour through eco-efficient services : An empirical study of car sharing in the Nerherlands. Bus. Strategy Environ. **1998**, 7, 234–244.
2. Shaheen, S.A.; Cohen, A.P. Growth in worldwide carsharing: An international comparison. Transp. Res. Rec. J. Transp. Res. Board **2007**, 1992, 81–89.
3. Fellows, N.; Pitfield, D. An economic and operational evaluation of urban car-sharing. Transp. Res. D Transp. Environ. **2000**, 5, 1–10.
4. Nikolian, A.; Firouz, Y.; Gopalakrishnan, R.; Timmermans, J.-M.; Omar, N.; van den Bossche, P.; van Mierlo, J. Lithium ion batteries—Development of advanced electrical equivalent circuit models for nickel manganese cobalt lithium-ion. Energies **2016**, 9, 360.
5. Le, D.; Tang, X. Lithium-ion battery state of health estimation using Ah-V characterization. In Proceedings of the Annual Conference of Prognostics and Health Management (PHM) Society, Montreal, QC, Canada, 20–23 June 2011.
6. Marra, F.; Træholt, C.; Larsen, E.; Wu, Q. Average behavior of battery-electric vehicles for distributed energy studies. In Proceedings of the 2010 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT Europe), Gothenburg, Sweden, 11–13 October 2010.
7. Magnor, D.; Gerschler, J.B.; Ecker, M.; Merk, P.; Sauer, D.U. Concept of a battery aging model for lithium-ion batteries considering the lifetime dependency on the operation strategy. In Proceedings of the European Photovoltaic Solar Energy Conference, Hamburg, Germany, 21–25 September 2009.
8. Cars 21. How to Reduce EV Production Costs? EV Battery Tech USA. 2011. Available online: http: //www.cars21.com/news/view/670 (accessed on 18 October 2016).

УДК 004.052.42

ІВАНОВ В.Г.

МЕТОД ВІДНОВЛЕННЯ ДАНИХ З ЗАДАНОГО ЧИСЛА СЕКТОРІВ ДИСКА З ВИКОРИСТАННЯМ ЗВАЖЕНИХ КОНТРОЛЬНИХ СУМ

В роботі запропоновано метод резервування та відновлення даних на магнітних носіях з використанням зважених контрольних сум. Висока ефективність запропонованого методу забезпечується використанням частково-ортогональних кодів в якості вагових коефіцієнтів. Розроблено алгоритм отримання таких кодів. Детально викладені математична ідея та процедури відновлення даних, доступ до яких втрачено. Розроблений метод ілюстровано прикладами. Наведено теоретичні та експериментальні оцінки запропонованого методу. Розроблений метод має на меті забезпечення високого рівня надійності систем розподіленого зберігання даних.

In this work, a method for backup and restoring data on magnetic disc by weighed checksum using has been proposed. The high efficiency of the proposed method is achieved by using of partial-orthogonal codes. Algorithm for obtained of such codes have been worked out. The mathematical idea of proposed method and procedure for recovering of data from access lost storage unit are described in details. A numerical example for developed recovering procedure are given. The theoretical and experimental effectiveness evaluation of the proposed method is demonstrated as well. The proposed method is aimed to ensure a high level of survivability of system of distributed data storage.

1. Вступ

До теперішнього часу накопичувачі на жорстких магнітних дисках займають домінуюче становище. За даними [1], на частку жорстких дисків припадає близько 95% інформації, що зберігається в комп'ютерних системах, решта (5%) даних зберігається на CD, CD-R, CD-RW дисках і флеш-носіях.

Швидкий розвиток інформаційних технологій має наслідком багатократне збільшення ємкості магнітних дисків, ускладнення їх структури. При цьому має місце тенденція до випередження збільшення ємкості дисків в порівнянні зі зростанням надійності. Це має призводить до того, що збільшується ймовірність виходу з ладу окремих секторів диску. При цьому слід розрізняти дефектність сектору на етапі його виготовлення. Ці сектори при форматуванню маркуються і їх використання в процесі експлуатації диску блокується. Іншим видом відмов – є пошкодження структури магнітного матеріалу під час експлуатації. В літературі [1] відмічається важлива особливість: з розвитком нових технологій виготовлення магнітних дисків їх сектори частіше виходять з ладу під час експлуатації.

Таким чином, актуальною задачею для сучасних технологій зберігання інформації є розробка ефективних методів та засобів відновлення інформації з секторів диску, яка втрачена в результаті фізичних процесів або програмних помилок.

2. Огляд методів відновлення даних на дисках

Проблема забезпечення надійного доступу до даних, що містяться на магнітних дисках спонукала до створення ряду технологій резервування.

Найбільш простою схемою резервування є використання простого дублювання даних на двох носіях. До такого типу відносяться системи Intermemory [2] та RAID-1 [3]. Використання простого дублювання пов’язане зі значними затратами об’єму пам’яті. При цьому, воно не гарантує відновлення даних при втраті доступу до обох носіїв, на яких зберігаються копії даних.

Значно меншого об’єму пам’яті потребує схема резервування, що передбачає для групи носіїв використання одного контрольного, на якому зберігається сума за модулем 2 відповідних даних всіх носіїв групи. Ця схема дозволяє доволі просто відновити дані при втраті доступу до одного

з носіїв групи. Найбільш відомим застосуванням описаної схеми резервування є система RAID-1 [3]. Проте ця схема не дозволяє відновлювати дані при втраті доступу до більш як одного носія.

Найбільшого поширення на практиці набули технології відновлення даних на основі коригуючих та erasure кодів [4]. При відновленні даних з носіїв, до яких втрачено доступ, як правило, не має потреби в їх локалізації. Класичні коригуючі коди, такі, як коди Хемінга, БЧХ, Ріда-Соломона орієнтовані на послідовне виконання двох процедур: локалізації спотвореної частини даних та їх виправлення. З цієї причини при використанні згаданих вище класичних коригуючих кодів для відновлення даних з носіїв, до яких втрачено доступ, потрібна їх модифікація. Модифіковані коди Ріда-Соломона, зокрема, використовуються в системі відновлення даних з носіїв RAID-6 [3].

Більш ефективно використання для цієї цілі спеціальних erasure кодів. Більшість таких кодів [4] мають за основу лінійні перетворення, і це зумовлює швидке зростання кількості резервних носіїв при збільшенні числа носіїв до яких втрачено доступ.

Загальною рисою відомих технологій відновлення даних з носіїв, до яких втрачено доступ є те, що вони потребують значних об'ємів додаткової пам'яті.

Ціллю досліджень є розробка та дослідження методу відновлення даних з окремих секторів магнітних дисків, який дозволяє зменшити об'єм резервної памяті.

3. Метод відновлення даних з секторів магнітного диску

Нехай інформація зберігається на n носіях. Блок, який зберігається на кожному з носіїв складається з m секторів.

У найпростішому випадку можна вважати, що ймовірність втрати інформації на секторі дорівнює p. Якщо для відновлення використовується один додатковий накопичувач, кожен із секторів якого формується як сума по модулю два однойменних секторів всіх n основних накопичувачів, то відновлення j-того сектора, де $j \in \{1,..,m\}$, буде неможливим тільки в разі, якщо пошкоджені j-ті сектора не менше, ніж двох з $n + 1$ накопичувачів. Відповідно, ймовірність того, що j-тий сектор всіх носіїв не пошкоджений становить $(1-p)^{n+1}$, а ймовірність, того, що пошкоджений j-тий сектор тільки одного з $n + 1$ накопичувачів дорівнює: $n \cdot p \cdot (1-p)^n$. Таким чином, ймовірність того, що з $n + 1$ накопичувачів не більше ніж в одному пошкоджений j-тий сектор становить суму наведених вище ймовірностей: $(1-p)^{n+1} + n \cdot p \cdot (1-p)^n$. Враховуючи, що на практиці значення p вельми малі, то для оціночних розрахунків цілком можна враховувати тільки компоненти, які містять мінімальну ступінь p, нехтуючи компонентами, що містять більш високі ступені p. Виходячи з цього: $(1-p)^{n+1} \approx 1+(n+1) \cdot p$ и $n \cdot p \cdot (1-p)^n \approx n \cdot p - n^2 \cdot p^2$,так, что $(1-p)^{n+1} + n \cdot p \cdot (1-p)^n \approx 1 - n^2 \cdot p^2$.

Імовірність P_1 того, що може бути відновлений будь-який з m секторів кожного з n накопичувачів, визначається ймовірністю того, що кожен з m секторів пошкоджений не більше ніж на одному з $n + 1$ накопичувачах: : $P_1 = ((1-p)^{n+1} + n \cdot p \cdot (1-p)^n)^m \approx (1-n^2 \cdot p^2)^m$. Таким чином: $P_1 \approx (1-n^2 \cdot p^2)^m = 1-m \cdot n^2 \cdot p^2$.

З цього випливає, що при використанні одного додаткового носія ймовірність відновлення інформації лінійно залежить від ємності (m) окремого носія. У той же час, залежність зазначеної ймовірності від числа n носія носить квадратичний характер.

Експериментально доведено, що при використанні трьох систем контрольних сум, з імовірністю 100% відновлюється до 5 секторів.

Більш ефективним є використання для відновлення даних зважених контрольних сум.

Зміст запропонованого методу полягає в тому, що для виправлення наперед заданого числа k секторів дискового накопичувача пропонується використовувати k систем вагових коефіцієнтів, як це показано на рис.1.

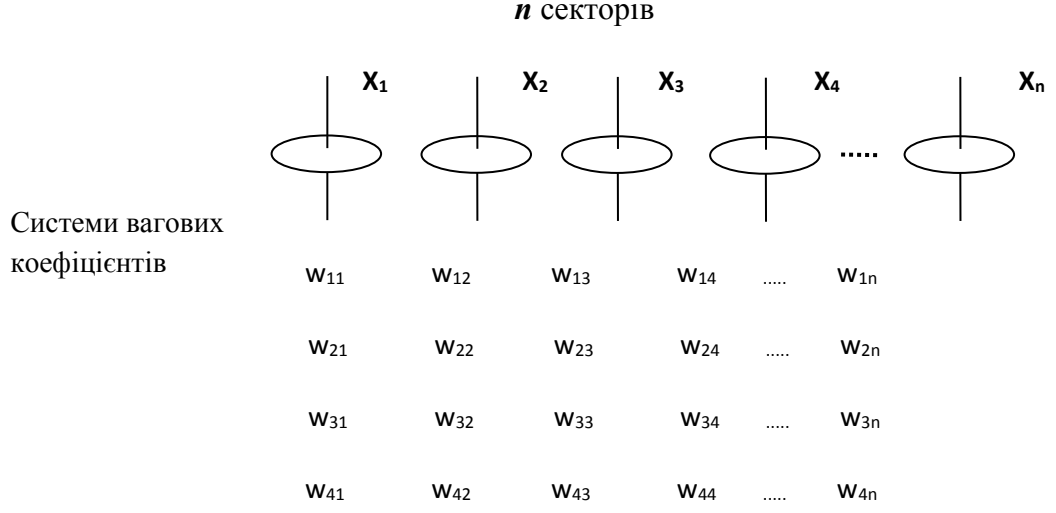

Рис.1 Використання систем вагових коефіцієнтів для відновлення даних секторів диска.

Відповідно, для відновлення даних з k секторів використовуються k контрольних кодів, що обчислюються як суми по модулю 2 добутків без переносів (логічний або поліноміальний добуток) вагових коефіцієнтів на коди даних:

$$X_1 \otimes w_{11} \oplus X_2 \otimes w_{12} \oplus \ldots \oplus X_n \otimes w_{1n} = C_1$$
$$X_1 \otimes w_{21} \oplus X_2 \otimes w_{22} \oplus \ldots \oplus X_n \otimes w_{2n} = C_2$$
$$X_1 \otimes w_{31} \oplus X_2 \otimes w_{32} \oplus \ldots \oplus X_n \otimes w_{3n} = C_3 \quad (1)$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$X_1 \otimes w_{k1} \oplus X_2 \otimes w_{k2} \oplus \ldots \oplus X_n \otimes w_{kn} = C_k$$

При втраті доступу до будь-яких k-тих секторів носія, обчислюються нові значення зважених контрольних сум, які сумуються по модулю 2 зі значеннями збережених контрольних сум. В результаті сумування формуються значення $\Delta C_1, \Delta C_2, \ldots, \Delta C_k$. Тоді процес відновлення зводиться до вирішення наступної системи лінійних рівнянь:

$$X_i \otimes w_{1i} \oplus X_j \otimes w_{1j} \oplus \ldots \oplus X_q \otimes w_{1q} = \Delta C_1$$
$$X_i \otimes w_{2i} \oplus X_j \otimes w_{2j} \oplus \ldots \oplus X_q \otimes w_{2q} = \Delta C_2$$
$$X_i \otimes w_{3i} \oplus X_j \otimes w_{3j} \oplus \ldots \oplus X_q \otimes w_{3q} = \Delta C_3 \quad (2)$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$X_i \otimes w_{4i} \oplus X_j \otimes w_{4j} \oplus \ldots \oplus X_q \otimes w_{4q} = \Delta C_k$$

Спеціальна процедура вибору системи вагових коефіцієнтів забезпечує можливість вирішення системи рівнянь при будь-яких значення i, j, k, q. Крім операцій множення без переносів, запропонований метод використовує операцію ділення P/Y $2 \cdot m$-розрядного числа P на m-розрядне число Y. Ця операція відповідає ділення поліномів. Результат цієї операції складається з частки - Q(P/Y)та залишку R(P/Y), так, що P=Q(P/Y)$\otimes Y \oplus$ R(P/Y). Наприклад, якщо P = $1011100=92_{10}$, а $Y=1001=9_{10}$, то першому з цих чисел співвідноситься поліном $x^6+x^4+x^3+x^2$, а другому - x^3+1. Відповідно, при діленні зазначених поліномів формується частка x^3+x і залишок x^2+x. Таким чином, Q(P/Y) = 1010, а R(P/Y) = 0110, так, що P= 1010⊗1001+110 = 1011100.

Визначення вагового коефіцієнта $W_j = \{w_{j,1}, w_{j,2}, \ldots, w_{j,q}\}$, $j \in \{1,\ldots,N\}$ на основі відомих: вектора $E=\{e_1, e_2, \ldots, e_m\}$, бітових спотворень і коду $\Delta_2=\{\delta_1, \delta_2, \ldots, \delta_q\}$ різниць може бути зведено до розв'язання системи лінійних рівнянь. Заданий нерозкладний поліном $P(x)$ поля Галуа визначає лінійну функцію $\lambda_1(w_{j,1}, w_{j,2}, \ldots, w_{j,q})$ отримання q-тої бітової компоненти $w_{j+1,q}$ вагового коефіцієнта W_{j+1} наступного носія: $w_{j+1,q}=\lambda_1(w_{j1}, w_{j2}, \ldots, w_{jq})$, в той час, як перші його q-1 компоненти являють собою зсунуті компоненти коефіцієнта W_j : $w_{j+1,1}=w_{j,2}$, $w_{j+1,2}=w_{j,3}, \ldots$, $w_{j+1,q-1}=w_{j,q}$ так , що $W_{j+1} = \{w_{j2}, w_{j3}, \ldots, w_{jq}, \lambda_1(w_{j1}, w_{j2}, \ldots, w_{jq})\}$. Наприклад, при $P(x) = x^4 + x + 1$ лінійна функція $\lambda_1=w_{j,1} \oplus w_{j,4}$. Якщо $W_{11}=\{1,1,0,0\}$ то $W_{12}=\{1,0,0, 1\oplus 0\}$. Аналогічно, $W_{j+2} = \{w_{j,3}, w_{j,4}, \ldots, w_{j,q}, \lambda_1(w_{j,1}, w_{j,2}, \ldots, w_{j,q}), \lambda_1(w_{j,2}, \ldots, w_{j,q}, \lambda_1(w_{j,1}, w_{j,2}, \ldots, w_{j,q}))\}$. Якщо позначити лінійну функцію

$\lambda_1(w_{j,2},...,w_{j,q},\lambda_1(w_{j,1},w_{j,2},...,w_{j,q}))$ як функцію $\lambda_2(w_{j,1},w_{j,2},...,w_{j,q})$, то $W_{j+2}=\{w_{j,3},w_{j,4},...,w_{j,q}, \lambda_1(w_{j,1},w_{j,2},...,w_{j,q}),\lambda_2(w_{j,1},w_{j,2},...,w_{j,q})\}$. Так в рамках розглянутого прикладу $\lambda_2 = w_{j,2} \oplus\lambda_1(w_{j,1},...,w_{j,4}))=w_{j,2}\oplus w_{j,1}\oplus w_{j,4}$, відповідно ваговий коефіцієнт W_{13} можна представити у вигляді: $W_{13}=\{w_{11,3},w_{11,4},w_{11,1}\oplus w_{11,4},w_{11,2}\oplus w_{11,1}\oplus w_{11,4}\} = \{0,0,1\oplus0,\ 1\oplus1\oplus0\}=\{0,0,1,0\}$. Виконавши аналогічні міркування і ввівши відповідні позначення, можна прийти до висновку про те, що бітові компоненти вагового коефіцієнта W_{j+m} останнього блоку даних можуть бути представлені у вигляді лінійних функцій від компонент вагового коефіцієнта W_j першого біта "пачки":

$W_{j+m}=\{w_{j,m},...,w_{j,q}, \lambda_1(w_{j,1},...,w_{j,q})$,..., $\lambda_{m-1}(w_{j,1},...,w_{j,q})\}$ при $m<q$

$W_{j+m}=\{w_{j,q},\lambda_1(w_{j,1},...,w_{j,q}),...,$ $\lambda_{q-1}(w_{j,1},...,w_{j,q})\}$ при $m=q$ (3)

$W_{j+m}=\{\lambda_{m-q+1}(w_{j,1},...,w_{j,q}),...,$ $\lambda_m(w_{j,1},...,w_{j,q})\}$ при $m>q$

Кожна l-та, де $l=2,...,m-1$, лінійна функція λ_l рекурсивно виражається через раніше визначені функції: λ_1 $\lambda_2,...,\lambda_{l-1}$ наступним чином:

$\lambda_l(w_{j,1},...,w_{j,q}) = \lambda_1(w_{j,i},...,w_{j,q}, ,\lambda_1(w_{j,1},...,w_{j,q}),..., \lambda_{l-1}(w_{j,1},...,w_{j,q})).$ (4)

$e_1\cdot w_{j,1} \oplus e_2\cdot w_{j+1,1} \oplus e_3\cdot w_{j+2,1} \oplus,...,$
$\oplus e_m\cdot w_{j+m,1} = \delta_1$.

Вираз (4) може бути узагальненим і для всіх інших компонент $\delta_2,...,\delta_q$ різниці Δ_2, і-та, і = $i=1,...,q$ компонента δ_i різниці Δ_2 являє собою логічну суму i- тих компонент вагових коефіцієнтів тих носіїв, доступ до яких втрачено. Отже, можна скласти q рівнянь виду:

$$e_1 \cdot w_{j,1} \oplus e_2 \cdot w_{j+1,1} \oplus e_3 \cdot w_{j+2,1} \oplus \cdots$$
$$\oplus e_m \cdot w_{j+m,1} = \delta_1$$
$$e_1 \cdot w_{j,2} \oplus e_2 \cdot w_{j+1,2} \oplus e_3 \cdot w_{j+2,2} \oplus \cdots$$
$$\oplus e_m \cdot w_{j+m,2} = \delta_2$$

....

$$e_1 \cdot w_{j,q} \oplus e_2 \cdot w_{j+1,q} \oplus e_3 \cdot w_{j+2,q} \oplus \cdots$$
$$\oplus e_m \cdot w_{j+m,q} = \delta_q \qquad (5)$$

З урахуванням того, що кожна з компонент вагових коефіцієнтів W_{j+1}, W_{j+2}, ..., W_{j+m} може бути виражена як лінійна функція від компонент вагового коефіцієнта W_j, всі рівняння системи (5) можуть бути лінійно виражені через компоненти $w_{j,1}$, $w_{j,2}$,..., $w_{j,q}$ коефіцієнта W_j. Отже, система (5) може бути представлена у вигляді системи q лінійних рівнянь від q бінарних невідомих $w_{j,1}$, $w_{j,2}$,..., $w_{j,q}$ для ситуації коли $m\geq q$ наступним чином:

$$e_1 \cdot w_{j,1} \oplus e_2 \cdot w_{j,2} \oplus \cdots \oplus e_m \cdot$$
$$\lambda_{m-q+1}(w_{j,1},.., w_{j,q}) = \delta_1$$
$$e_1 \cdot w_{j,2} \oplus e_2 \cdot w_{j,3} \oplus \cdots \oplus e_m \cdot$$
$$\lambda_{m-q+2}(w_{j,1},.., w_{j,q}) = \delta_2$$

....

$$e_1 \cdot w_{j,q} \oplus e_2 \cdot \lambda_1(w_{j,1},.., w_{j,q}) \oplus$$
$$\cdots \oplus e_m \cdot \lambda_m(w_{j,1},.., w_{j,q}) = \delta_q \qquad (6)$$

Якщо $m<q$, то система (6) може бути представлена як система лінійних рівнянь в наступному вигляді:

$$e_1 \cdot w_{j,1} \oplus e_2 \cdot w_{j,2} \oplus \cdots \oplus$$
$$e_m \cdot w_{j,m} = \delta_1$$
$$e_1 \cdot w_{j,2} \oplus e_2 \cdot w_{j,3} \oplus \cdots \oplus$$
$$e_m \cdot w_{j,m+1} = \delta_2$$

....

$$e_1 \cdot w_{j,q-m+1} \oplus e_2 \cdot w_{j,q-m+2} \qquad (7)$$
$$\oplus \cdots \oplus e_m \cdot w_{j,q} = \delta_{q-m+1}$$
$$e_1 \cdot w_{j,q-m+2} \oplus e_2 \cdot w_{j,q-m+3}$$
$$\oplus \cdots \oplus e_m \cdot \lambda_1(w_{j,1},.., w_{j,q}) = \delta_{q-m+2}$$

....

$$e_1 \cdot w_{j,q} \oplus e_2 \cdot \lambda_1(w_{j,1},.., w_{j,q})$$
$$\oplus \cdots \oplus e_m \cdot \lambda_{m-1}(w_{j,1},.., w_{j,q}) = \delta_q$$

Системи (6) і (7) можуть бути досить просто вирішені відомими способами і, як результат, отримані значення двійкових компонент $w_{j,1}$, $w_{j,2}$,..., $w_{j,q}$ вагового коефіцієнта W_j носія.

4. Висновки

В результаті проведених теоретичних і експериментальних досліджень, спрямованих на підвищення ефективності відновлення даних, що зберігаються на пошкоджених фрагментах носія (сектора)

запропонований метод відновлення даних з заданих секторів носія, доступ до яких втрачено, відмінністю якого є використання системи зважених контрольних сум із спеціально вибраними ваговими коефіцієнтами, що дозволяє зменшити обсяг використовуваної додаткової пам'яті в порівнянні з відомими методами.

Література

1. Коженевский СР. Безопасность хранения информации на жестких дисках : - Зб. наук. праць НАН України, 2003 р. №4 . - С. 67-84.
2. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение / Р. Морелос-Сарагоса.- М.: Техносфера, 2005.- 319 с.
3. Reed I.S.. Polynomial codes over certain finite fields / I.S. Reed, G. Solomon // Journal of the Society for Industrial and Applied Mathematics.-1960.- № 8(2). - pp. 300–304.
4. Wickers S.B.. Reed-Solomon Codes and Their Applications / S.B.Wickers, V.K. Bhargava - IEEE Press. Piscataway, New Jersey.-1983.- p.433

УДК 681.325

КРАВЧУК А.А.
САВЕРЧЕНКО В.Г.

УНИФИКАЦИЯ ВЫЧИСЛЕНИЙ В ПРОБЛЕМНО-ОРИЕНТИРОВАННЫХ КОНВЕЙЕРНЫХ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМАХ

Рассматриваются вопросы унификации вычислений в проблемно-ориентированных конвейерных вычислительных системах на основе введения обобщенной процедуры, эквивалентной последовательности базовых операций. При этом любая операция рассматривается как частный случай выделенной обобщенной процедуры, получаемой на основе системы правил подстановок. Это достигается путем доопределения потоков данных при помощи подстановки в обобщенную процедуру нулей и единиц вместо тех значений операндов, которые не определены в заданной операции. Введение в машинный язык обобщенных процедур рассматривается как предпосылка для повышения эффективности проблемно-ориентированных вычислительных систем.

The questions of unification of computing in problem-oriented conveyor computer systems based on the introduction of a generalized procedure, the equivalent sequence of basic operations. At the same time, any operation is considered as a special case of the isolated generalized procedure, obtained on the basis of the system of rules of substitutions. This is achieved by adding data streams by substituting zeros and ones for the generalized procedure instead of those values of operands that are not defined in the specified operation. Introduction to the machine language of generalized procedures is considered as a prerequisite for improving the efficiency of problem-oriented computing systems.

Ключевые слова: проблемно-ориентированные конвейерные вычислительные системы, унификация вычислений, обобщенная процедура.

1. Введение

При построении современных высокопроизводительных вычислительных средств обработки информации широкое распространение получили конвейерные и матричные процессоры, использующие совмещение и распараллеливание операций соответственно.

В конвейерных процессорах, каждая строка конвейера перед началом либо во время вычислений настраивается на выполнение определенной операции. В матричных процессорах процессорные элементы работают параллельно и выполняют одну и ту же операцию.

Для повышения эффективности вычислений при решении широкого круга задач необходимо организовать связи между процессорными элементами таким образом, чтобы наиболее полно обеспечить загрузку процессорных элементов. При этом разнообразие выполняемых операций усложняет как систему управления вычислениями, так и в ряде случаев уменьшает производительность системы в целом [1].

2. Постановка задачи

Представляется актуальным поиск таких системотехнических решений, которые позволяли бы реализовать обработку информации, эффективно сочетающих совмещение и распараллеливание операций, и учитывающих специфику конкретного применения [2].

Один из наиболее эффективных подходов к построению проблемно-ориентированных вычислительных систем (ПОВС), базируется на унификации вычислений и связан с выбором минимального набора базовых операций, реализующих оптимальным образом любую задачу, принадлежащую данному классу.

В общем случае алгоритм решаемой задачи может быть представлен в виде последовательности элементов, принадлежащих к множеству допустимых операторов входного языка ПОВС. При

этом каждому оператору ставится в соответствие определенная группа одиночных команд внутреннего языка, которые обычно называются машинными командами.

Каждая машинная команда определяет выполнение одной из множества базовых многоместных операций, эквивалентных некоторой последовательности бинарных операций. Иными словами, выполняется отображение $S: A_i \to B^{(i)}$, где $B^{(i)} = \{B_1^{(i)}, \ldots, B_r^{(i)}, \ldots, B_{N^{(i)}}^{(i)}\}$ – последовательность базовых операций, соответствующая оператору A_i; $B_r^{(i)} = \{B_{r,l}^{(i)} \mid l = \overline{1, N^{(r)}}\}$ – базовая многоместная операция, эквивалентная последовательности $N^{(r)}$ бинарных операций; r и l – порядковые номера базовой и бинарной операций в цепочке операций соответственно; $B^{(i)} \in B$ ($i = \overline{1, N}$, $r = \overline{1, N^{(i)}}$).

3. Методика выделения обобщенных процедур

С унификацией вычислений будем связывать такое сокращение машинных команд, определенных для конкретной ПОВС, при котором длина последовательности базовых операций не увеличивается. В предельном случае ($M = 1$) каждому оператору входного языка ПОВС ставится в соответствие одна и та же обобщенная машинная команда, которая определяет операцию вычисления некоторой обобщенной процедуры (ОПР), эквивалентной последовательности базовых операций. При этом любая i-я операция, выполняемая в ПОВС, рассматривается как частный случай выделенной ОПР, получаемой на основе i-ой системы правил подстановок. Это достигается путем доопределения потоков данных при помощи соответствующих подстановок в ОПР кодов операндов из множества {0,1} вместо тех значений операндов, которые не определены в заданной операции. Другими словами, при унификации вычислений осуществляется отображение $S': A_i \to L^{(i)}$, где $L^{(i)}$ – i-я реализация ОПР L, аргументами которой могут быть как переменные, так и постоянные величины, причем $L = \{L_i \mid t = \overline{1, K}\}$ – цепочка K бинарных операций, вызываемых обобщенной машинной командой.

Введение ОПР позволяет унифицировать способ выполнения операций, а с ним и процесс вычислений в ПОКС. Однако для реализации этой возможности необходимо учитывать специфические особенности ОПР, к которым в первую очередь следует отнести относительно высокую ее сложность.

Степень сложности ОПР, определяемая числом бинарных операций, составляющих эквивалентную последовательность, может достигать. Поэтому при выборе структуры ПОВС следует учитывать возможности выполнения с ее помощью сложных вычислений. В этой связи для эффективной организации вычислений в ПОВС необходимо обеспечить выполнения следующего условия: $T(L) \approx T(B_r^{(i)})$, где $T(L)$ $T(B_r^{(i)})$ – время выполнения ОПР и базовых операций соответственно, $r = \overline{1, N^{(i)}}$, $i = \overline{1, N}$. К структурам, удовлетворяющих данному условию, относятся ПОВС, основанные на конвейерном методе обработки информации.

Унификация вычислений в конвейерных ПОВС определяет необходимость специальных преобразований для оптимального отображения операций из заданного набора в эквивалентную им ОПР.

Методика этих преобразований включает следующее:

– выделение ОПР из заданного набора операций;

– приведение ОПР к виду, удобному для реализации в ПОВС;

– минимизацию требуемой избыточности вычислений;

– реализацию ОПР в ПОВС.

Операции, выполняемые в ПОВС, приводятся к одной из следующих схем вычислений:

$$\sum_{i=1}^{n} A_i \prod_{j=1}^{n-i+1} \frac{X_j}{Y_j} \qquad (1),$$

$$\sum_{i=1}^{n}\prod_{j=1}^{k}\frac{X_{i,j}}{Y_{i,j}} \quad (2),$$

$$\prod_{i=1}^{n}\sum_{j=1}^{k}\frac{X_{i,j}}{Y_{i,j}} \quad (3),$$

$$B_0+\bigcup_{i=1}^{n}\frac{A_i}{B_i} \quad (4),$$

где символы $\bigcup_{i=1}^{n}\frac{A_i}{B_i}$ определяют сокращенную запись цепной дроби.

Реализация схемы вычислений (1), (2), (3) или (4), наиболее близкой по структуре к выбранным ОПР, осуществляется на основе конвейерных ПОВС, допускающих организацию вычислений в автономном, полуавтономном и неавтономном режимах [3].

4. Заключение

Рассмотренная организации вычислений позволяет процесс выполнения операций сделать однотипным и легко реализовать его аппаратурными средствами. Использование конвейерных процессоров, настроенных на оптимальное выполнение ОПР, соответствующих специфике конкретного применения, существенно повышает производительность и уровень внутренних языков конвейерных ПОВС.

Это обусловлено, прежде всего тем, что реализация ОПР на уровне машинного языка позволяет:

– осуществить реализацию многоместных операций;

– сократить объемы оперативной памяти для представления программ;

– сократить количество обращений к памяти, необходимых для реализации соответствующих алгоритмов обработки данных;

– управление выполнением операций свести к формированию начальных условий.

Недостатком унификации вычислений на основе ОПР является некоторое недоиспользование процессорных ресурсов ПОВС, так как данный подход предполагает избыточность применительно к конкретным вычислениям. Однако благодаря успехам в области интегральной технологии и возможности уменьшения избыточности за счет расширения набора ОПР указанный недостаток можно считать несущественным.

Таким образом, введение ОПР во внутренний язык конвейерных ПОВС создает предпосылки для дальнейшего повышения производительности вычислительных средств, расширения средств внутренних языков, обеспечения наиболее эффективного использования оперативной памяти и существенного упрощения вопросов организации вычислений.

Список литературы

1. Представление задач в системах распараллеливания с изменяемой зернистостью/ Г. М. Луцкий, С. Г. Стиренко, А. И. Зиненко, Д. В. Грибенко // Вісн. Нац. техн. ун-ту України "КПІ". Сер. Інф-ка, упр. та обчисл. техніка. - 2012. - Вип. 55. - С. 11-17.

2. Самофалов К. Г., Луцкий Г. М. Основы теории многоуровневых конвейерных вычислительных систем Радио и связь Москва 1989 271 с.

3. Самофалов К. Г., Луцкий Г. М. Основы построения конвейерных ЭВМ. Киев: Вища шк. Головное изд-во. 1981. 224 с.

УДК 004.04

КАЛЮЖНИЙ І.Г.,
ДУБІНСЬКИЙ Є.В.

МЕТОД ТА ЗАСОБИ ВЕРИФІКАЦІЇ ТА ВІДОБРАЖЕННЯ СТАТИСТИЧНИХ ДАНИХ В КАРТОГРАФІЧНОМУ ФОРМАТІ

В даній статті було розглянуто метод верифікації картографічних даних з послідуючим відображенням на мапі на прикладі сервісу для оренди нерухомості. Для прикладу була обрана локація міста Києва та всіх його районів. Також було проведено порівняльну характеристику засобів досягнення даної мети та їх опис. Засоби відображення та верифікації порівнювались по параметрам швидкодії і простоті у використанні.

This article examined the method of verification mapping data with subsequent display on a map. As the example service for rental was picked. Kyiv and all its regions location were selected as a territory example. It was also conducted comparative characterization of tools which was needed to achieve this goal. These mapping and verification tools were compared by performance and “ease to use” parameters.

1. Вступ

В даній статті зроблено огляд методу верифікації статистичних даних з послідуючим наданням їм картографічного формату і послідуючого відображення на мапі. Для демонстрації універсальності методу було обрано місто Київ та всі його регіони. Статистичні дані а також всі довготи і широти було взято з ресурсів які знаходяться у вільному доступі в мережі Інтернет.

2. Огляд засобів верифікації і відображення даних

Для збереження статистичних даних було обрано формат JSON, так як цей формат найбільше підходить для збереження даних у картографічному вигляді. Виходячи з даних умов, для верифікації даних було обрано технологію для валідації JSON Schema. JSON Schema це потужний інструмент для перевірки структури даних JSON. Детальну інформацію по даному інструменту та його використанню можна знайти в [1]. Також було обрано технологію jQuery validation plugin, який дозволяє верифікувати дані на стороні користувача. Застосунок для відображення обирався серед додатків Яндекс.Карты, 2ГИС та Google Maps. З недоліків Яндекс.Карт можна відзначити відсутність деталізації на рівні будівель, відсутність відображення у режимі 3D та слабке покриття міст і регіонів по всьому світу. Перевагами даного застосунку є найкраще покриття території Росії і наявність режиму «нічний». 2ГИС карти мають гарну деталізацію об’єктів але слабке покриття у всьому світі. Google Maps покривають весь світ на високому рівні деталізації. Так як 2ГИС і Яндекс.Карты поступаються Google Maps в більшості порівняльних характеристик (покриття світу, деталізація відображення), а універсальність і точна робота методу націлена на будь-яку територію, то було обрано Google Maps API[2] як технологію відображення картографічних даних. Детальну порівняльну характеристику наведено у табл. 1.

3. Верифікація статистичних даних та надання їм картографічного вигляду

Збір статистичних даних по нерухомості відбувається один раз на день за допомогою виконання сценарію який створено на мові PHP. Він розбирає та аналізує відповідний ресурс в мережі Інтернет. Об’єкт аналізу має бути обрано коректно і відповідно до місцевості, інакше буде колізія між даними і відображуваною територією. Після аналізу відбувається верифікація отриманих даних. Для прискорення

роботи алгоритму верифікації, дані розбиваються на лексеми, які потім одна за одною перевіряються на наявність синтаксичних помилок, наявність необхідної інформації та помилок що могли статися за рахунок людського фактору під час внесення даних. Після верифікації дані зберігаються у базі даних, попередньо набувши картографічного формату. Цей формат досягається за допомогою додавання до статистичних даних довготи і широти місцевості якій ці дані належать.

4. Метод відображення картографічних даних

На початку роботи програми відображається початкова обрана місцевість (для демонстрації була обрана територія міста Київ) поділена на райони. На областях районів відображається базова статистична інформація. Координати початкової території та його районів отримуються за допомогою сервісу openstreetmap[3], а статистична інформація завантажується в результаті роботи PHP-сценарію.

Також на головному екрані присутні налаштування по відображенню даних, наприклад можна показати найдорожчі варіанти нерухомості або приховати квартири, число кімнат у яких менше за задану кількість та ін.

При натисканні на район, мапа змінюється і відображає обраний район у повному розмірі, а інформація по нерухомості стає детальнішою. Також на користувацькому інтерфейсі присутній набір фільтрів, які дають змогу показувати лише деякі із можливих даних. Фільтри не можна конфігурувати з інтерфейсу користувача, але їх можна змінювати, видаляти чи створювати у програмному коді додатку.

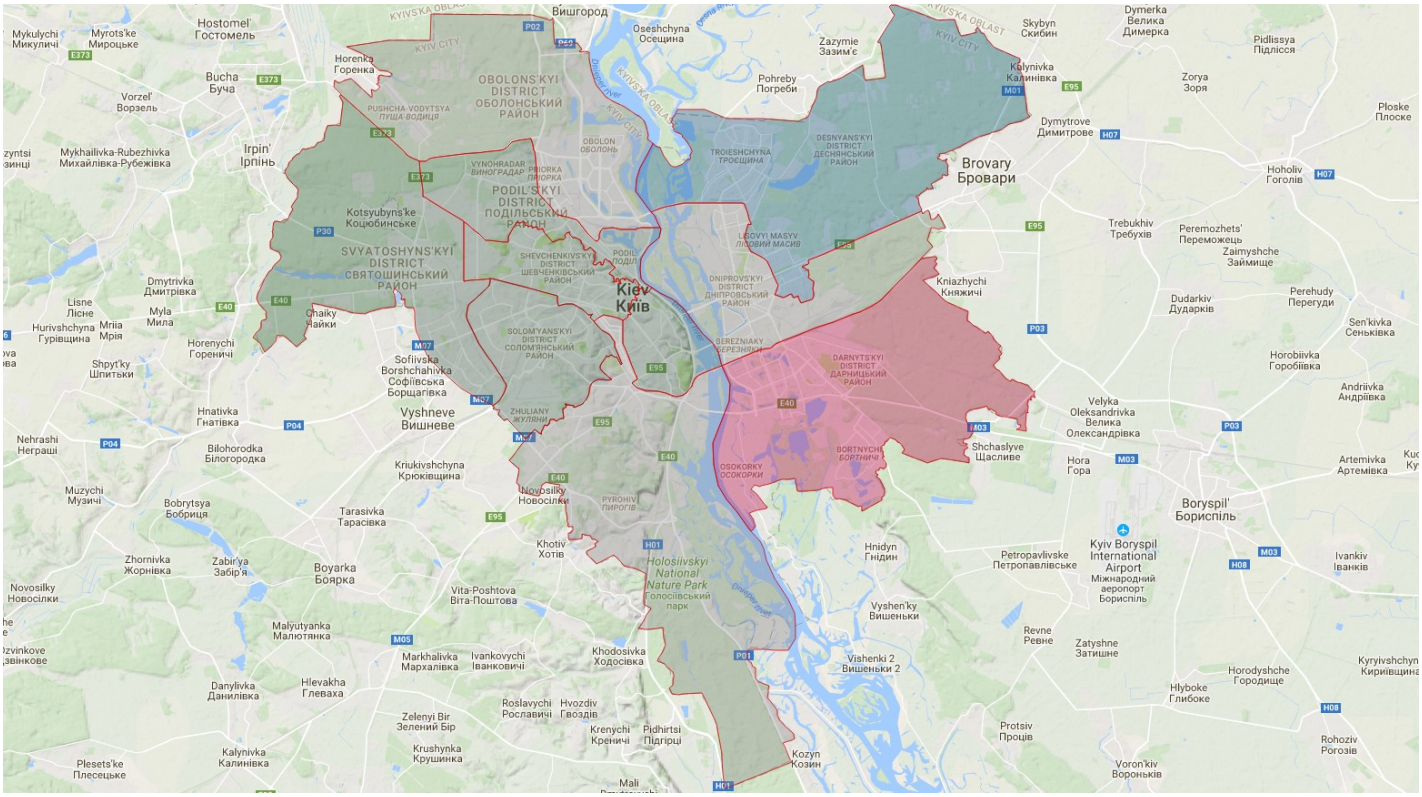

Рис. 1. Приклад інтерфейсу користувача з відображенням мапи Києва

Табл 1. Порівняльна характеристика засобів відображення картографічних даних.

Критерій порівняння	Яндекс.Карты	2ГИС	Google Maps
Покриття	Краще покриття Росії, поступається Google в покритті світу	Поступається конкурентам в покритті як в Росії, так і в інших країнах	Краще покриття всього світу
Деталізація	Хороша деталізація Росії, достатня в світі	Одна з кращих деталізацій в містах присутності	Хороша деталізація по всьому світу. На карті Росії можуть бути відсутні великі міста. У плані відображення невиразна деталізація. Об'єкти добре видно тільки при досить сильному наближенні.
Деталізація на рівні будівель	Нема	Великі торгові центри	Великі торгові центри
Можливість завантаження і використання офлайн	Є. Великий розмір даних	Є	Є. Великий розмір даних
Режим 3D	Однакова висота будівель	Є	Є
Висновок	Добре знає географію і організації по всій Росії. Наявність сервісів «Народна карта», «Панорами вулиць», голосового введення	Детальна інформація по організаціям і висока деталізація карт в містах присутності	Зручне і функціональне побудова маршрутів. Панорама вулиць, голосове введення

5. Висновки

На прикладі сервісу по нерухомості було продемонстровано метод для верифікації статистичних даних, перетворення даних у картографічний формат і відображення їх на мапі. Даний метод відображає обране місто і його райони (в даному прикладі розглядалося місто Київ) а також статистику у сфері оренди жилого приміщення. Також є можливість проглянути детальну інформацію по обраному району. На виді всього міста відображається загальна інформація по районам, а на виді детального огляду району відображається об'єкти для оренди та інформація по ним. Також є можливість фільтрації даних які відображаються. За допомогою обраних користувачем критерій виводиться специфічна інформація. Досить великий набір фільтрів (наприклад сортування по ціні, кількість кімнат, поверх, та ін.) робить систему досить гнучкою у використанні. Суть методу полягає у можливості відображати різну територію та статистику до неї представляючи необхідну інформацію. Для зміни локації відображення потрібно зробити запит з назвою бажаного міста до сервісу openstreetmap. В результаті буде завантажена інформація по обраній місцевості та її розподіл на райони. Також для коректної роботи потрібна статистика по нерухомості. В даному прикладі статистика береться з ресурсу Інтернет. Її оновлює і аналізує PHP-сценарій один раз на день. Сценарій можна налаштувати на сканування будь-якого ресурсу Інтернет. Це дозволить отримувати статистику для потрібного міста та його районів.

Список літератури

1. Michael Droettboom Understanding JSON Schema. – 2016 – С. 10 – 24.
2. Gabriel Svennerberg Beginning Google Maps API – 2010 – С. 45 – 100.
3. Yu-Wei Lin A qualitative enquiry into OpenStreetMap making – 2011.

УДК 004.048

КАПЛУНОВ А.В.
СІМОНЕНКО А.В.

ПОБУДОВА БАЄСОВСЬОЇ МЕРЕЖІ ДОВІРИ ДЛЯ КЛАСИФІКЦІЇ ЗАХВОРЮВАННЯ

У статті розглянуто практичне застосування баєсової мережі довіри для класифікації хвороби пацієнта, ґрунтуючись на симптоматиці його захворювання. Описана методика генерації структури статичних моделей баєсових мереж довіри за експериментальними вибірками значень змінних та принцип їх функціонування.

Ключові слова: баєсова мережа довіри, таблиці умовних ймовірностей, причинно-наслідкові зв'язки.

The article deals with the practical application of Bayesian believe network to classify the patient ill based on the symptoms of his disease. This workaround structure generation static models Bayesian believe network for the experiment variables and how they function.

Keywords: Bayesian believe network, table of conditional probabilities, the cause-effect relationships.

1. Вступ

Завдання класифікації представляє собою завдання віднесення зразка до однієї з декількох множин, що попарно не перетинаються. Прикладом таких завдань може бути, завдання визначення кредитоспроможності клієнта банку, рішення задач управління портфелем цінних паперів, завдання визначення життєздатних і схильних до банкрутства фірм.

Логічним наслідком цього є те, що нейронні мережі можливо використовувати з метою діагностування найбільш ймовірного захворювання пацієнта, ґрунтуючись на симптоматиці його захворювання.

Для цих цілей пропонується застосувати баєсову мережу довірі.

2. Огляд баєсової мережі довіри в загальному вигляді

Баєсова мережа довіри - використовується в областях, які можна охарактеризувати успадкованою невизначеністю. Причиною цієї невизначеності може бути:

- неповнота знань;
- випадковість характеризації завдання;
- неповнота розуміння предметної області.

Отже, баєсові мережі довіри (БМД) доцільно застосовувати для моделювання ситуацій в яких має місце певна невизначеність. Баєсові мережі довіри іноді називають причинно-наслідковими мережами, в яких випадкові події поєднані причинно-наслідковими зв'язками.

З'єднання методом причин і наслідків дозволяє відносно легко оцінити ймовірність події. У реальному світі оцінка зазвичай робиться в напрямку від "спостерігача" до "спостереження" або від "ефекту" до "наслідку". В цьому випадку провести оцінку значно важче, ніж при спостереженні від “наслідку” до “ефекту”, тобто в напрямку від наслідку.

Таким чином, баєсові мережі довіри (БМД) надають дослідникам можливість використовувати зручне графічне представлення багатовимірних статистичних розподілів. Теорема Баєса, яка лежить в основі БМД, дає можливість визначити ймовірність виконання певної події (гіпотези), коли ми володіємо лише непрямими підтвердженнями (даними), які можуть бути не точними, і визначає формулу Баєса:

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)}$$

де P (A|B) - ймовірність гіпотези A при настанні події B (апостеріорна ймовірність); P (B|A) - ймовірність настання події B при істинності гіпотези

A; P (A) - апріорна ймовірність гіпотези A; P (B) - ймовірність настання події B.

3. Теоретичне підґрунтя теореми Баєса

Формула Баєса дозволяє за відомим фактом події обчислити вірогідність того, що вона була викликана даною причиною. Події, які є наслідками дії «причини», називаються гіпотезами, оскільки вони є передбачуваними подіями, що викликані даними. Безумовна ймовірність справедливості гіпотези називається апріорною (яка ймовірність причини взагалі), а умовна з урахуванням факту настання подія - апостеріорною (наскільки ймовірною виявилися причина обліку даних про подію) [1].

Важливим наслідком формули Баєса є формула повної ймовірності події, що залежить від декількох несумісних гіпотез:

$$\mathrm{P(B)} = \sum_{i=1}^{N} \mathrm{P}(A_i)\mathrm{P}(\mathrm{B}|A_i),$$

де P (A_i) - ймовірність i-ї гіпотези; P (B|A_i) - ймовірність настання події B при істинності гіпотези A.

Баєсові мережі довіри являють собою сп рямований ациклічний граф, що має насту пні властивості:

- кожну вершину представляють як п одію, яку можна описати випадковою вели чиною, і що може мати декілька станів;
- вершини які мають "батьківські" ви значені у таблиці умовних ймовірностей (Т УЙ)

або у функції умовних ймовірностей (ФУЙ);

- вершини без "батьків", мають безум овні (маргінальні) ймовірності своїх станів .

Тобто, у баєсових мережах довіри вершини є відображенням випадкових змінних, а дуги - ймовірнісних залежностей, які визначаються через таблиці умовних ймовірностей. Таблиця умовних ймовірностей кожної вершини містить інформацію про ймовірність стану цієї вершини в залежності від стану її "батьків".

Якщо на графі БМД ребро виходить з вершини A у вершину B, то вершину A називають батьківською по відношенню до B, а B - нащадком по відношенню до A. Спільний розподіл значень в вершинах можна зручно розписати як результат локальних розподілів у кожному вузлі і в його предків:

$$P(X_1, X_2, \dots, X_n) = \prod_{i=1}^{n} P(X_i|par(X_i)),$$

де X_i - ймовірність події в вершині i; par (X_i) - безліч предків вершини X_i.

Якщо у вершини Xi немає "батьків", то її локальний розподіл ймовірностей називають безумовним, у іншому випадку він є умовним. Якщо значення в вузлі отримано в результаті досвіду, то вершину називають свідком (позначену вершиною подію - свідченням).

Таким чином, БМД дозволяють точно формалізувати причинно-наслідкові зв'язки, які відбуваються всередині будь-якої системи, в тому числі при діагностування найбільш ймовірного захворювання пацієнта, ґрунтуючись на симптоматиці його захворювання.

4. Аналіз структури взаємозв'язків показників БМД

Основним завданням при побудові БМД, що моделює реальний процес, є встановлення структури взаємозв'язків показників. При цьому результатом спостереження таких процесів є набір значень експериментальних даних (навчальна вибірка):

$$D=\{d_1,d_2,\dots,d_n\}, d_i=\{x_{i1},x_{i2},\dots,x_{iN}\},$$

де d_1, d_2, ..., d_n - спостереження за станом показників; n - кількість спостережень; x_{i1}, x_{i2}, ..., x_{iN} - стан змінних показників його спостереження; N - кількість показників, що беруть участь в спостереженні.

Оскільки повний перебір всієї безлічі нециклічних моделей, і вибір з них найбільш відповідної навчальної вибірки, має NP-важку обчислювальну складність - для вирішення такого завдання застосовувати його не є доцільним.

Таким чином, побудова баєсової мережі необхідно проводити евристичним методом. Для цього в першу чергу необхідно визначити структуру взаємозв'язків вершин, встановивши їх взаємний вплив в контексті аналізованого процесу. Другим етапом побудови є

навчання мережі - тобто привласнення ваг взаємозв'язкам, встановлення умовних ймовірностей.

Для вирішення першого завдання, з огляду на специфіку і складність поставленого завдання, одним з кращих варіантів є побудова структури баєсової мережі з використанням досвіду експертів в даній області знань. Збір думки експертів про взаємні зв'язки показників і їх вплив на надійність проводиться у вигляді анкетування та спільної побудови графічної моделі за результатами анкетування. Однак варто враховувати, що людський фактор негативно впливає на точність оцінки, і, незважаючи на достатню кількість методик підвищення об'єктивності отриманих даних, вони можуть використовуватися лише для побудови чернетки графа взаємозв'язків баєсової мережі [2].

5. Оцінка ступеня взаємозв'язку пар змінних

Для оцінки ступеня взаємозв'язку пар змінних в безлічі показників надійності зручно використовувати значення обопільної інформації, яке пов'язане з поняттями ентропії та умовної ентропії. Для дискретної випадкової величини ентропія з функцією розподілу p (x) = p (X - x) визначається як

$$H(X) = -\sum_x p(x) \log\, p(x).$$

У свою чергу, умовна ентропія для пари дискретних випадкових величин Y і X при відомому X визначається як

$$H(Y|X) = \sum_x p(x) H(Y|X = x) =$$

$$= -\sum_x p(x) \sum_y p(y|x) \log\, p(y|x) =$$

$$= -\sum_x \sum_y p(x,y) \log\, p(y|x)$$

Отже, для випадків коли Y пов'язаний з X функціональною залежністю, H (У | X) = 0. Для всіх x: p (x)> O, значення Y визначається як y = g (x), з ймовірністю p (y | x) = 1.

Так звана mutual information показує кількість інформації, яку одна випадкова змінна містить про іншу. Для двох випадкових змінних X і Y зі спільною функцією розподілу p (x, y) обопільна інформація MI (X, Y) - це відносна ентропія, фактично аналог кореляції, але для інформаційних показників [3]

$$MI(X,Y) = \sum_x \sum_y p(x,y) \log \frac{p(x,y)}{p(x)p(y)} =$$

$$= H(Y) - H(Y|X) = H(X) - H(X|Y)$$

MI = 0 в тому випадку, коли оцінювані показники (вершини графа БМД) є незалежними одна від одної, так як

$$p(x,y) = p(x)p(y),$$

$$\log \frac{p(x,y)}{p(x)p(y)} = \log \frac{p(x)p(y)}{p(x)p(y)} = \log 1 = 1.$$

Таким чином, MI > 0 показує наявність обопільної інформації, або інформаційної залежності, між вершинами. Підрахувати p (x) для кожної з вершин за наявною експериментальною вибіркою нескладно, при зростанні обсягу даних точність збільшується.

У разі, якщо БСД складається з N вершин, для обчислення MI між усіма парами вершин потрібно виконати (N (N-1)) / 2 обчислень, при цьому MI (x, y) = MI (y, x).

6. Висновок

Отримані за допомогою обчислень результати спільно з побудованим за результатами експертного аналізу «каркасом» БСД дозволяють отримати коректний граф, що відображає статистичні взаємозв'язки показників з надійністю ПЗ.

Початкові умовні ймовірності для вершин задаються на підставі рекурсивної формули. Їх коригування на більш пізніх етапах можливе, коли в результаті збору показників виходить нова повністю заповнена вибірка d_1. В ході подальшої роботи мережі граничні маргінальні вершини, відповідно до вимірюваних в ході оцінки метрик, максимізують значення ймовірностей, що відповідають вимірюваним показникам (тобто для вершини і $p_i (x_j) = 1$ у разі, коли $X_i = x_j$).

Таким чином, використовуючи описану методику побудови і навчання баєсової мережі, для отримання об'єктивної оцінки діагностування найбільш ймовірного захворювання пацієнта, ґрунтуючись на симптоматиці його захворювання, дослідникам залишається лише зібрати достатню кількість експериментальних даних. Згенерована модель дозволить отримувати прогнози надійності високого ступеня довіри і об'єктивності.

Список літератури

1. Heckerman D. A tutorial on learning with Bayesian networks. The MIT Press, Cambridge, Massachusetts, 1998.

2. Kahneman D., Slovic P., Tversky A. Judgment Under Uncertainty: Heuristics and Biases. Cambridge: University Press, Cambridge, 1982.

3. Chow C.K., Liu C.N. Approximating discrete probability distributions with dependence trees // IEE Transactions on information theory. Vol. IT–14. № 3. 1968.

УДК 004.056.53

КУКСА В. В.
ЖАБІН В. І.,

МЕТОД ВИЯВЛЕННЯ АТАК НА ОСНОВІ СТАТИСТИЧНОГО АНАЛІЗУ ПОКАЗНИКІВ ЗАВАНТАЖЕННЯ СИСТЕМИ

У даній статті розглянуто виявлення вторгнень із використанням статистичного аналізу показників завантаження системи. Досліджено підхід до підвищення точності виявлення аномальної поведінки із застосуванням результатів одночасного спостереження декількох різних показників завантаження системи. Була показана ефективність запропонованого методу для виявлення певних типів атак.

The subject of this paper is an intrusions detection based on statistical analysis of the system load characteristics. The approach to increase the accuracy of abnormal behavior detection using the simultaneous observation of several different system load characteristics was studied. The proposed method was shown to be efficient at detection of certain types of attacks.

1. Вступ

Важливість проблеми захисту інформації зростає із стрімким розвитком комп'ютерних технологій. Впровадження комп'ютерних мереж у таких сферах, як фінансова, виробнича, охорони здоров'я, роблять комп'ютерні системи привабливою ціллю для атак і великою вразливістю для суспільства.

Традиційно, захист комп'ютерних систем будується із застосуванням таких засобів як, шифрування, мережеві екрани (файрволи), віртуальні приватні мережі і т. п., але цього недостатньо для забезпечення повної безпеки. У зв'язку з цим постає необхідність у розробці динамічних засобів, що здатні вести постійний аудит системи і реагувати на несанкціоновану діяльність. Для вирішення цієї задачі були створені системи виявлення атак (СВА).

Дані які вказують на несанкціоновану діяльність можуть надходити із широкого різноманіття джерел: мережеві служби, журнали подій операційної системи (ОС) і користувацького програмного забезпечення (ПЗ) і т. і. Об'єм цих даних може бути дуже великим, а методи їх аналізу — мати високу обчислювальну складність. Тому постає проблема вибору найбільш ефективних джерел вхідних даних для СВА.

У даній роботі наведена характеристика сучасних типів СВА, проаналізовані потенційні проблеми джерел даних для СВА. Запропоновано підхід для підвищення точності виявлення атак на основі даних про рівень завантаження системи до задовільного рівня.

2. Типи систем виявлення атак

В залежності від джерела вхідних даних, розрізняють два основних типи систем виявлення атак: хостові та мережеві.

Хостові системи виявлення атак (ХСВА) встановлюються на окремі машини. СВА цього типу аналізують різні аспекти поведінки захищеної системи, такі як: мережеві з'єднання хоста (RealSecure Agent), цілісність файлової системи (Tripwire, AIDE), журнали подій (LogSentry), взаємодія програмного забезпечення із ядром операційної системи [1].

При своїй високій ефективності хостові СВА мають і суттєві недоліки. Перший недолік випливає з того, що СВА встановлено безпосередньо на хості, що може бути атакований, а отже, джерела інформації, якими користується СВА, можуть бути скомпрометовані. Наприклад, техніка приховування системних викликів описана у [2]. Якщо СВА працює не в реальному часі, засоби знищення системних журналів та інших слідів втручання, що входять до складу сучасних інструментів проникнення, таких як Metasploit Framework, також дозволяють уникнути виявлення атаки [3]. Іншим недоліком існуючих хостових СВА є високі витрати ресурсів захищеної системи на збір

інформації (журналювання подій, перехоплення системних викликів, трафіку тощо) і її обробку.

Мережеві системи виявлення атак (МСВА) спираються на дані про використання локальної мережі. МСВА збирають і аналізують усі пакети, що надійшли на інтерфейс шлюза або мережевого адаптера, що працює у нерозбірливому режимі (захоплює усі пакети, а не лише ті, що призначені для нього) [1]. Так як МСВА обробляє не тільки пакети, адресовані певному хосту, вона забезпечує захист цілому сегменту мережі [1].

Розгортання і адміністрування МСВА простіше за ХСВА, але платою за це стає обмеження інформації, доступної системі для аналізу, лише мережевим трафіком. Об'єм трафіку, що протікає у сучасних локальних мережах, сягає від десятків мегабіт до десятків гігабіт за секунду і аудит всіх пакетів вимагає значних обчислювальних ресурсів. Вибірковий же аналіз пакетів збільшує шанси на пропуск проявів атаки. Із впровадженням шифрування трафіку МСВА або втрачають можливість аналізу вмісту пакетів, або повинні розшифровувати трафік, створюючи тим самим нову потенційну точку атаки на шифрований трафік.

При розгляді сучасних типів систем виявлення атак і використовуваних ними джерел даних були виявлені певні проблеми із їх застосуванням. Особливо варто відзначити проблему достовірності і доступності вхідних даних. Також, відкриття таких джерел інформації, як наприклад шифрованого трафіку у мережі для СВА, робить саму СВА додатковим вразливим місцем системи.

3. Показники завантаження системи

Усі сучасні операційні системи (Windows, UNIX-подібні) у процесі виконання своїх функцій, отримують у розпорядження вичерпну інформацію про завантаженість усіх апаратних і програмних компонентів.

Для вирішення нашої задачі було обрано наступні показники завантаження: час центрального процесора (ЦП), використаний процесом на рівні користувача, час ЦП, використаний процесом на рівні ОС (виконання системних викликів), об'єм пам'яті процесу, кількість потоків процесу, кількість байтів, зчитаних з диску і записаних на диск, кількість файлів, відкритих процесом, кількість вхідних і вихідних мережевих пакетів для кожного сокета, відкритого процесом.

4. Набори даних

У дослідженні використовувалась дані, зібрані під час роботи загальновикористовуваних програм, різних за розміром і складністю, як в умовах нормального використання, так і при різних типах втручання («відмова в обслуговуванні», «виконання стороннього коду»). Інструменти втручання було взято із бази даних вразливостей https://www.exploit-db.com.

Кожен набір даних являє собою послідовність записів із значеннями вибраних показників завантаження системи одним процесом від початку його виконання до завершення, зафіксованими через рівні проміжки часу в 1 секунду.

Дані для сервера баз даних MySQL були зібрані для нормальної поведінки під змінним навантаженням, що симулювалося за допомогою утиліти mysqlslap [4], та при втручанні типу "виконання стороннього коду" під час роботи під змінним навантаженням. Вразливість, що використовувалась для втручання, зареєстрована під ідентифікатором CVE-2016-6662.

Збір даних для сервера додатків Apache Tomcat виконувався аналогічним чином. Для симуляції навантаження застосовувалася утиліта siege [5]. Втручання у роботу сервера було виконано із використанням вразливості типу "відмова в обслуговуванні". Вразливість зареєстрована під ідентифікатором CVE-2014-0050.

Для задачі навчання методів моделювання було використано приблизно 50% даних нормальної поведінки обох програм.

5. Побудова моделі нормальної поведінки

Метод, що пропонується, спирається на дані, які складно підробити у разі проникнення; їх генерація не вимагає змін у користувацькому ПЗ (журналювання подій)

і додаткових ресурсів системи, що захищається.

Показники завантаження несуть багато інформації про стан процесу, але складно визначити, чи є зміна окремих показників нормальною чи аномальною, адже вона може залежати від дуже великої кількості умов. Наприклад, використання ЦП і пам'яті веб-сервером різко зростає при надходженні запитів від клієнтів і знижується майже до нуля при відсутності запитів.

Проте, спостереження дозволяють встановити, що співвідношення між певними показниками залишаються незмінними при нормальній роботі програми. Виходячи з цього, для побудови моделі нормальної поведінки програми, необхідно знайти зв'язані показники і визначити характер співвідношення між ними.

У математичній статистиці наявність і сила взаємозв'язку величин характеризується кореляцією і її мірою є коефіцієнт кореляції r [6]. У нашому випадку будемо шукати кореляцію між послідовностями значень пар показників завантаження системи програмою у часі. Так як усі показники є кількісними змінними, застосуємо лінійний коефіцієнт кореляції [6]. Перед побудовою моделі обирається порогове значення коефіцієнта кореляції $r_{\text{п}}$, при перевищенні якого вважається, що між парою показників існує зв'язок.

Виявивши зв'язані показники, необхідно знайти характер залежності між ними. Для спрощення вважатимемо залежність між ними лінійною, а отже, можемо застосувати метод найменших квадратів для обчислення коефіцієнтів лінійної регресії [7].

Отже, база даних нормальної поведінки програми складається із пар пов'язаних показників і коефіцієнтів лінійної регресії, що описує зв'язок між ними.

6. Тестування поведінки програми

У процесі тестування через задані інтервали на основі поточного значення кожного показника у базі даних нормальної поведінки обчислюється значення відповідного пов'язаного показника. Для різниці між реальним значенням показника і обчисленим за даними бази нормальної поведінки встановлене порогове значення Δ, при перевищенні якого реєструється неспівпадіння. Оскільки показники можуть мати дуже різні границі виміру, їх значення нормується із урахуванням цих границь, що є або фіксованими (використання ЦП), або можуть бути отримані від ОС (об'єм пам'яті, максимальна кількість відкритих файлів), або визначені емпірично в процесі формування профілю нормальної поведінки. Завдяки цьому, можна задати єдине порогове значення Δ.

На кожному кроці перевірка однієї пари показників вимагає константного часу. Отже, загальний час перевірки на кожному кроці пропорційний $O(P)$, де P - кількість пар зв'язаних показників у базі даних.

Для боротьби із хибно позитивних результатів необхідно враховувати декілька неспівпадінь. Як правило, під час реальних атак аномальна активність проявляється на коротких проміжках часу. Тому мірою аномальності поведінки було обрано кількість неспівпадінь n на фіксованому проміжку часу t. В кожен момент тесту підтримується інформація про те, скільки неспівпадінь спостерігалося за минулий проміжок часу фіксованої тривалості.

Для міри аномальності встановлюється поріг N, до якого поведінка програми вважається нормальною. Щоразу, коли міра досягає або перевищує поріг, фіксується атака. Поріг різниці між очікуваним значенням показника і реальним Δ і міри аномальності N є головними регуляторами чутливості методу. Нижчі порогові значення ведуть до збільшення успішно виявлених атак, але також і збільшення кількості хибно позитивних спрацьовувань, і навпаки, вищий поріг зменшує кількість як істинно позитивних так і хибно позитивних результатів.

7. Результати дослідження

Ми протестували кожен із трьох методів моделювання на кожному з наборів даних при декількох різних порогах чутливості. Хибно позитивні результати підраховувались для частини даних нормальної поведінки, не використаної в процесі навчання, а істинно позитивні – для записів аномальної поведінки.

Метод показав дуже відмінні результати на кожному з наборів даних. На рисунку 1

представлені середні результати для кожної комбінації набору даних порогу чутливості. Вісь ординат на рисунку 1 показує загальну здатність методу до виявлення аномалій. Вісь абсцис показує частоту хибно позитивних результатів. Частота хибно позитивних результатів визначена як відношення кількості хибно позитивних результатів до загальної кількості вимірів за час тестування нормальної поведінки, і її значення лежить у діапазоні від 0 до 1.

Невелика частка виявлених атак типу "виконання стороннього коду" пояснюється ти, що зловмисницький код не впливає суттєво на функціювання ураженої програми. В той же час, точність виявлення атак типу "відмова в обслуговуванні" є задовільною, оскільки порушення основної функції програми внаслідок вторгнення веде до суттєвих змін у споживанні нею системних ресурсів.

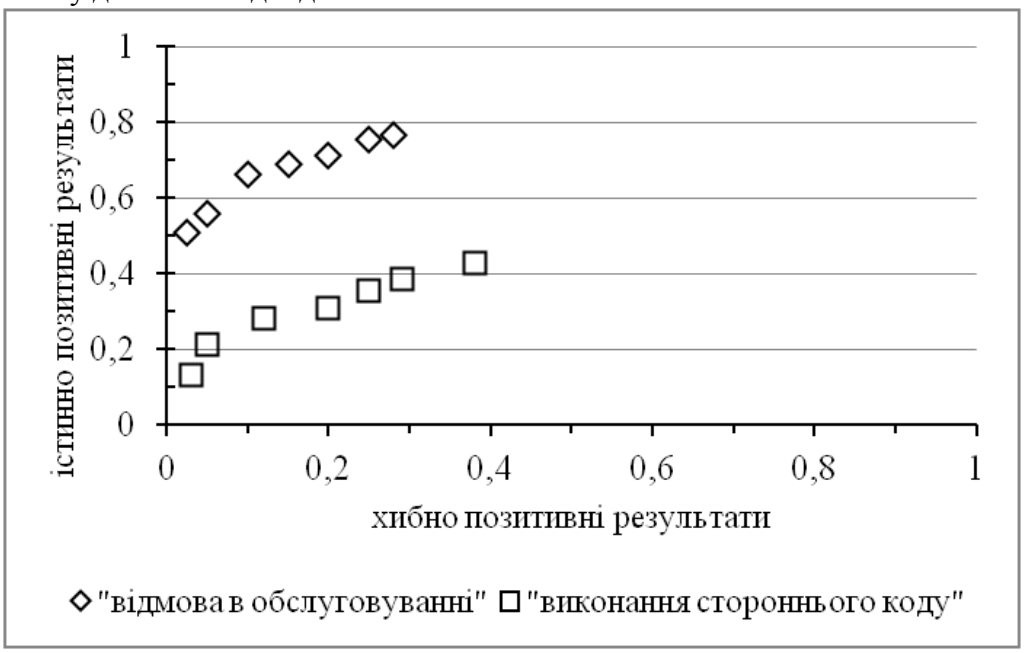

Рис. 1. Об'єднані результати для типів атаки «відмова в обслуговуванні» і «виконання стороннього коду»

8. Висновки

Запропонований підхід до використання показників завантаження системи для вирішення задачі виявлення вторгнень має наступні переваги: висока достовірність і доступність вхідних даних, висока швидкість обробки даних та незалежність методу від типу комп'ютерної системи та її застосування.

Розроблений метод був протестований на наборах даних, що відповідають різним програмам і технікам вторгнення. Метод показав невисоку ефективність проти атак типу "виконання стороннього коду". У той же час, була досягнута задовільна точність виявлення атак типу "відмова в обслуговуванні", що пояснюється суттєвими змінами у споживанні атакованою програмою системних ресурсів.

Таким чином, запропонований метод дозволяє підвищити точність виявлення певних типів вторгнень на основі показників завантаження системи.

Список літератури

1. Kazienko P. Intrusion Detection Systems (IDS) Part 2 – Classification; methods; techniques [Електронний ресурс] / P. Kazienko, P. Dorosz // TechGenix Ltd.. – 2004. – Режим доступу до ресурсу: http://techgenix.com/ids-part2-classification-methods-techniques/.

2. Srivastava A. System Call API Obfuscation (Extended Abstract) / A. Srivastava, L. Andrea, G. Jonathon // Recent Advances in Intrusion Detection – 11th International Symposium, RAID 2008, Cambridge, MA, USA, September 15-17, 2008, Proceedings / A. Srivastava, L. Andrea, G. Jonathon.

– Berlin Heidelberg: Springer-Verlag, 2008. – (Security and Cryptology; т. 5230). – С. 421 – 422.

3. Event Log Management [Електронний ресурс] // Offensive Security. – 2015. – Режим доступу до ресурсу: https://www.offensive-security.com/metasploit-unleashed/event-log-management/.

4. mysqlslap — Load Emulation Client [Електронний ресурс] // Oracle Corporation. – 2017. – Режим доступу до ресурсу: https://dev.mysql.com/doc/refman/5.7/en/mysqlslap.html.

5. Fulmer J. Siege Manual [Електронний ресурс] / Jeffrey Fulmer. – 2012. – Режим доступу до ресурсу: https://www.joedog.org/siege-manual/.

6. Собственно-корреляционные параметрические методы изучения связи. Оценка существенности корреляции / Р. А.Шмойлова, В. Г. Минашкин, Н. А. Садовникова, Н. А. Шувалова // Теория статистики / Р. А.Шмойлова, В. Г. Минашкин, Н. А. Садовникова, Н. А. Шувалова. – Москва: Финансы и статистика, 2004. – С. 361–376.

7. Парная регрессия на основе метода наименьших квадратов и метода группировок / Р. А.Шмойлова, В. Г. Минашкин, Н. А. Садовникова, Н. А. Шувалова // Теория статистики / Р. А.Шмойлова, В. Г. Минашкин, Н. А. Садовникова, Н. А. Шувалова. – Москва: Финансы и статистика, 2004. – С. 333–342.

УДК 004.056.5

КУЦ В.Ю.,
ШАПРАН К.О.

ОРГАНІЗАЦІЯ ВИПРАВЛЕННЯ ПОМИЛОК СИНХРОНІЗАЦІЇ В ПОСЛІДОВНИХ ІНТЕРФЕЙСАХ КОМПЮТЕРНИХ СИСТЕМ

Доповідь присвячена проблемі підвищення ефективності корекції багатократних помилок синхронізації в послідовних каналах передачі даних комп'ютерних систем. У статті запропоновано, теоретично обґрунтовано та досліджено оригінальний метод формування контрольного коду та його використання для виправлення всіх помилок синхронізації, кратність яких не перевищує двох. Детально представлено математичну ідею методу та процедуру корекції помилок. Використання процедури корекції ілюструється прикладом. Наведено теоретичні та експериментальні оцінки ефективності запропонованого методу.

Доклад посвящен проблеме повышения эффективности коррекции многократных ошибок синхронизации в последовательных каналах передачи данных компьютерных систем. В статье предложен, теоретически обоснован и исследован оригинальный метод формирования контрольного кода и его использование для исправления всех ошибок синхронизации, кратность которых не превышает двух. Подробно представлено математическую идею метода и процедуру коррекции ошибок. Использование процедуры коррекции иллюстрируется примером. Приведены теоретические и экспериментальные оценки эффективности предложенного метода.

The presentation deals with problem of efficiency increase in correction of multiple synchronization errors in serial data transition channels in computer systems. New method of control code formation is offered, theoretically proved and analyzed in this article, as well as its use for correction of all synchronization errors multiplicity of which is not greater than two. It has detailed mathematical idea of this method and errors correction procedure. The use of correction procedure is illustrated in the example. The theoretical and experimental effectiveness evaluation of proposed method are given.

1. Вступ

Реаліями сьогоднішнього дня стало розширення використання розподілених обчислень і тенденція до “інтелектуалізації” периферійних пристроїв комп’ютерних систем, що має наслідком різке зростання об’ємів обміну даними. Разом з цим, постійно зростають і вимоги до швидкості передачі даних. Для прикладу, стандарт послідовного інтерфейсу SATA за останні десять років збільшив пропускну здатність у 5 разів, новий стандарт USB 3.0 порівняно з попередньою версією збільшує максимальну швидкість передавання даних відразу в 10 разів, до 5 Гбіт/с [1].

Збільшення швидкості передавання даних неминуче призводить до росту кількості помилок, адже саме передача даних залишається однією з найменш надійних частин комп’ютерних систем. Причиною цьому є низка складних фізичних процесів, що одночасно протікають в середовищі передачі, та призводять до викривлення та пошкодження інформації, що передається. І чим більша швидкість передачі даних застосовується, тим більше фізичних процесів та явищ здатні значно вплинути на процес передачі. Наприклад, при обміні інформацією по оптоволоконним каналам на швидкостях, що перевищують 10 Гбіт/с доводиться зіштовхуватися з новим ефектом, який не відіграє суттєвої ролі на маленьких швидкостях – поляризаційно-модовою дисперсією (PMD), суть якої полягає у тому, що дві поляризовані компоненти світлового імпульсу можуть рухатися із різними швидкостями та спотворювати сигнал. Крім того, при роботі з будь-яким фізичним середовищем передачі доводиться зіштовхуватися із завадами, здатними накладатися на дані, що передаються, та викривляти їх. Ці завади зазвичай є нерегулярними, невпорядкованими та структурно схожими на інформаційні сигнали, що ускладнює їх виявлення [2].

Таким чином, продиктована технічним прогресом необхідність постійного збільшення швидкостей передачі даних має компенсовуватись розробленням нових методів виявлення та корекції помилок, що дозволяють забезпечити ефективність та надійність передачі інформації на великих швидкостях.

Особливо гостро постає проблема забезпечення достовірності інформації, що передається, у обчислювальних системах та мережах, оскільки, на відміну від систем зв'язку або цифрового телебачення, така інформація може бути застосована для керування важливими об'єктами, відповідно до чого зростає ціна як втрати часу при повторному пересиланні даних, так і помилкового визнання пошкодженого пакету даних коректним, що може мати значні негативні наслідки [2].

Таким чином, задача підвищення ефективності виявлення та виправлення помилок синхронізації в асинхронних лініях обміну цифровими даними комп'ютерних систем є актуальною на сучасному етапі розвитку інформаційних технологій.

2. Аналіз існуючих засобів корекції помилок синхронізації

Для будь-якої сучасної обчислювальної системи, передача інформації є одним із базових процесів. Вона відбувається як між окремими вузлами комп'ютера, так і з віддаленими периферійними пристроями, або іншими системами. Для передачі цифрових даних на фізичному рівні розроблено низку методів кодування, таких як NRZ (Non-Return to Zero), AMI (Alternate Mark Inversion), Манчестерське кодування тощо. Недоліком багатьох методів є відсутність властивості самосинхронізації, тобто схильність до утворення помилок синхронізації [1].

Причина утворення помилок синхронізації гарно ілюструється механізмом роботи широковживаного в багатьох послідовних інтерфейсах (таких як USB або FireWire) способу кодування даних - NRZI (Non Return to Zero Invert – метод неповернення до нульового потенціалу). Даний метод використовує лише два види ділянок – з додатним потенціалом та протилежним від'ємним, без нульових областей, при чому передача біта нуля кодується зміною напруги в лінії, а при передачі одиниці значення напруги не змінюється [1].

Спосіб передачі даних окреслює можливі випадки виникнення помилок: якщо передавач надсилає довгу серію одиниць, то потенціал на лінії не змінюється протягом певного часу. Період синхронізації передавача τ_S відрізняється від періоду приймача τ_R на певну випадкову величину μ, так що $\tau_R = \tau_S + \mu$. При передачі серії з n одиниць, часовий інтервал на приймачеві може відрізнятися вже на $n \cdot \mu$, і якщо ця величина стає співрозмірною до τ_S, є певна ймовірність того, що приймач розпізнає серію з n одиниць, як таку, що містить n+1 або n-1.

Важливою особливістю помилок синхронізації є те, що традиційні механізми перевірки коректності даних, такі як використання надлишкових циклічних кодів (Cyclic Redundancy Codes, CRC), виявляються нездатними зафіксувати факт надходження пошкодженого інформаційного пакету [3]. CRC гарантує знаходження "пачки" помилок довжиною не більше степені утворюючого поліному, але оскільки в разі виникнення помилки синхронізації фактично доводиться мати справу зі зсувом надісланого блоку біт та зміною самого розміру отриманого пакета даних, CRC код в багатьох випадках пропускає пошкоджений блок, вважаючи його коректним.

Існує два механізми боротьби з помилками синхронізації: бітовий стаффінг та повторне надсилання пошкодженого помилкою блоку. Другий метод має багато недоліків: по-перше, ніяк не гарантується відсутність помилок у повторному повідомленні, по-друге, декількаразове надсилання одного й того ж самого блоку призводить до затримок у часі, що є суттєвим для систем з роботою у реальному часі [1].

Інший розповсюджений метод – бітовий стаффінг – дозволяє зменшити ймовірність виникнення помилок синхронізації шляхом додавання до кожної послідовності з шести поспіль одиниць нульового біту, тим самим зменшуючи час, протягом якого на лінії не змінюється потенціал. Подібний механізм ускладнює процес передачі та змушує передавати велику кількість додаткових байт

(до 17%), при цьому ніяк не гарантуючи відсутність помилок синхронізації, а тільки зменшуючи імовірності їх виникнення [4].

Існуючі корегуючи коди [4] для виправлення помилок синхронізації жорстко прив'язані з помилками, що виникають в USB, тобто зникненню лише одиниць. Разом з тим, на практиці використовується широкий арсенал методів низькочастотного кодування даних в яких помилки носять симетричний характер і кількість бітів, в результаті порушень синхронізації, може як збільшуватися, так і зменшувати.

Таким чином, існує необхідність в розробці спеціальних засобів виявлення та виправлення помилок синхронізації.

Разом з цим існує велика кількість застосувань для яких температури передавача та приймача істотно відрізняються та існує помітна ймовірність виникнення помилок, кратністю більше двох.

Таким чином, відомі методи не забезпечують ефективного вирішення задачі локалізації і корекції великої кількості одиночних та подвійних помилок синхронізації в темпі передачі даних.

Метою досліджень є розробка методу ефективної корекції одиночних та подвійних помилок синхронізації в темпі передачі цифрових даних між компонентами комп'ютерних систем з використанням асинхронних каналів.

3. Метод корекції помилок синхронізації

Для досягнення поставленої мети запропоновано метод корекції багатократних помилок синхронізації, що виникають у процесі передачі n-бітового блоку даних, який дозволяє суттєво розширити коригуючу здатність за рахунок виправлення однієї та двох помилок синхронізації, що виникають при передачі однієї послідовності несинхронізованих бітів.

Виникнення помилок синхронізації в процесі послідовної передачі цифрової інформації стає можливим тільки для фрагментів, що представляють собою послідовність несинхронізованих бітів, довжина l яких досягає певної критичної межі h. Ймовірність виникнення помилок синхронізації зростає зі збільшенням кількості послідовних несинхронізованих бітів у блоці даних. Тому в блоці даних B_S, що відсилається, виділяються всі фрагменти, що складаються з послідовності одиниць, довжиною не меншою за критичну межу $h_1 = 4$. Виділені фрагменти позначаються як E_{1S}, E_{2S}, …, E_{mS}, де m – кількість фрагментів у n-бітовому блоці B_S. Довжини фрагментів відповідно дорівнюють: l_{1S}, l_{2S}, …, l_{mS}, $\forall i = 1, \ldots, m$; $l_{iS} \geq h_1$. На стороні передавача пропонується сформувати контрольну послідовність S, яка складається з бітів $<c_1, c_2, c_3, \ldots, c_q>$, де $c_i \in \{0,1\}$, шляхом аналізу довжини l_{iS} фрагмента E_{iS}, де $i \in \{1,..,m\}$. Якщо довжина l_{iS} менша ніж $h_2 = 8$, то пропонується виділити два контрольних біти $<c_q, c_{q+1}>$, які обчислюються як залишок від ділення довжини виділеного фрагмента на чотири:

$$2 \cdot c_{q+1} + c_q = l_{iS} \bmod 4. \quad (1)$$

Якщо довжина послідовності несинхронізованих бітів більша критичної межі $h_2 = 8$, то в контрольну послідовність додаються три біти $<c_q, c_{q+1}, c_{q+2}>$, що обчислюються як залишок від ділення довжини l_{iS} фрагмента на вісім:

$$4 \cdot c_{q+2} + 2 \cdot c_{q+1} + c_q = l_{iS} \bmod 8. \quad (2)$$

Сформована описаним способом контрольна послідовність S передається разом з інформаційним блоком B_S до приймача.

На стороні приймача прийнятий блок даних $B_R = \{b_1, b_2, \ldots, b_n\}$, $\forall k \in \{1..n\}$: $b_k \in \{1, 0\}$, аналізується аналогічно до надісланого: виділяються фрагменти $E_{1R}, E_{2R}, .. E_{mR}$, що є послідовністю несинхронізованих бітів, кількість яких не менша за $h_1 = 4$. Кількість одиниць у цих фрагментах прийнятого блоку відповідно дорівнює: l_{1R}, l_{2R}, …, l_{mR}, $\forall i = 1, \ldots, m$; $l_{iR} \geq h_1$.

У прийнятому i-му фрагменті E_{iR} в залежності від довжини l_{iR} можуть виникати одна або дві помилки синхронізації. Запропонований метод враховує можливість виникнення двох помилок синхронізації у фрагментах, які представляють собою послі-довність несинхронізованих бітів, довжина l_{iR} яких більша за $h_2 = 8$: $l_{iR} \geq h_2$.

У фрагментах меншої довжини: $h_1 \leq l_{iR} < h_2$, $4 \leq l_{iR} < 8$ можливе виникнення помилок двох типів: поява додаткового одиничного біта, тобто збільшення отриманого фрагмента відносно відправленого на несинхронізований біт: $l_{iR} = l_{iS} + 1$, і втрата біта, що означає зменшення на несинхронізований біт прий-

нятого фрагмента відносно відправленого: $l_{iR} = l_{iS} - 1$.

При передачі більш довгих послідовностей несинхронізованих бітів, довжина l_{iR} яких більша за h_2: $l_{iR} \geq h_2$, $l_{iR} \geq 8$ існує ймовірність появи помилок синхронізації чотирьох типів: додавання одного несинхронізованого біту в процесі передачі, що призводить до збільшення довжини прийнятої послідовності відносно відправленої – $l_{iR} = l_{iS} + 1$; втрата одного біта, тобто зменшення кількості несинхронізованих бітів у прийнятому фрагменті в порівнянні з відправленим – $l_{iR} = l_{iS} - 1$; виникнення двох додаткових бітів, що означає збільшення довжини отриманого фрагмента відносно відправленого на два біти – $l_{iR} = l_{iS} + 2$; втрата двох несинхронізованих бітів, тобто зменшення на два біти прийнятого фрагмента у порівнянні з відправленим – $l_{iR} = l_{iS} - 2$.

Вирішення задачі виявлення помилок пропонується здійснювати шляхом порівняння та аналізу бітів отриманої контрольної послідовності від передавача та довжин виділених фрагментів несинхронізованих бітів на приймачі.

У розробленому методі аналізуються довжини l_{iR} фрагментів, що являються послідовністю несинхронізованих бітів на стороні приймача, щодо п’яти проміжків значень довжин. Усі проміжки сформовані відносно критичної межі $h_2 = 8$:

1) $l_{iR} < h_2 - 2$, якщо значення довжини l_{iR} фрагмента несинхронізованих бітів прийнятого блоку задовольняє умову, то перевіряються випадки передачі фрагмента безпомилково або з помилкою синхронізації одного з типів: додавання одного біта або втрата одного несинхронізованого біта при передачі. При виявленні помилки синхронізації пропонується виконати відповідну корекцію фрагмента шляхом вилучення або додавання одного біта;

2) $l_{iR} = h_2 - 2$, при виконанні умови, тоді перевіряється факт наявності помилки синхронізації. Передбачено можливість виник-нення помилки синхронізації одного з трьох типів: зменшення кількості одиниць на один/два біта або збільшення на один біт на стороні приймача фрагмента, що аналізується. Корекція відповідно реалізується шляхом додавання одного/двох бітів або вилучення одного несинхронізованого біта;

3) $l_{iR} = h_2 - 1$, якщо умова виконується, то пропонується перевірити випадок передачі фрагмента без помилок або з помилками синхронізації одного з трьох типів: втрата одного/двох несинхронізованих бітів або додавання одного біта при передачі фрагмента. Для корекції необхідно виконати збільшення фрагмента на один/два біта або зменшення на один несинхронізований біт;

4) $l_{iR} = h_2$, у випадку виконання умови, перевіряються випадки передачі фрагмента безпомилково або з помилкою синхронізації одного з трьох типів: додавання одного біта або втрата одного/двох несинхронізованих бітів при передачі. При виявленні помилки синхронізації пропонується виконати відповідну корекцію фрагмента шляхом вилучення або додавання одного/двох бітів;

5) $l_{iR} > h_2$, якщо значення довжини l_{iR} фрагмента задовольняє умову, тоді виконується перевірка на наявність помилки синхронізації або її відсутність. Передбачається можливість виникнення помилок чотирьох типів: змен-шення кількості несинхронізованих одиниць на один/два біта, або їх збільшення на один/два одиничних біта. У випадку виявлення помилки синхронізації виконуються корекції шляхом додавання/вилучення одного або двох несин-хронізованих бітів з фрагмента.

Формально, запропонований метод корекції багатократних помилок синхронізації представ-ляється у вигляді наступної послідовності дій:

1. У блоці даних B_S, що відсилається, виділяються фрагменти $E_{1S}, E_{2S}, \ldots, E_{mS}$, в яких кількість послідовних одиничних бітів не менша за h_1.

2. Визначається довжина l_{iS} кожного i-го фрагменту $E_{iS}, i \in \{1,2..m\}$, блоку.

3. Лічильник j фрагментів $E_{1S}, E_{2S}, \ldots, E_{mS}$, встановлюється в одиницю.

4. Індекс q поточного біту контрольної послідовності S встановлюється в одиницю.

5. Якщо довжина l_{jS} j-го фрагменту E_{jS} менша за h_2: $l_{jS} < h_2$, то в контрольну послідовність S додаються два біти $<c_q, c_{q+1}>$, які обчислюються як залишок від ділення

довжини l_{jS} на чотири: $2 \cdot c_{q+1} + c_q = l_{jS} \bmod 4$. Перехід на п.7.

6. Якщо довжина l_{jS} j-го фрагменту E_{jS} більша або дорівнює h_2: $l_{jS} \geq h_2$, то в контрольну послідовність S додаються три біти $<c_q, c_{q+1}, c_{q+2}>$, що обчислюються як залишок від ділення довжини l_{jS} на вісім: $4 \cdot c_{q+2} + 2 \cdot c_{q+1} + c_q = l_{jS} \bmod 8$. Перехід на п.8.

7. Індекс q збільшується на два: $q = q + 2$. Перехід на п.9.

8. Індекс q збільшується на три: $q = q + 3$.

9. Якщо $j < m$, то виконується інкремент значення лічильника: $j = j + 1$ і повернення на п.5.

10. Блок B_S передається разом із бітами $<c_1, c_2, c_3, \ldots, c_q>$ контрольної послідовності S.

11. У прийнятому блоці B_R виокремлюються фрагменти $E_{1R}, E_{2R}, .. E_{mR}$, що являють собою послідовності одиниць, довжиною не меншою за h_1.

12. Визначаються кількості $l_{1R}, l_{2R}, \ldots, l_{mR}$ одиниць у виділених фрагментах $E_{1R}, E_{2R}, .. E_{mR}$ прийнятого блоку.

13. Лічильник j фрагментів $E_{1R}, E_{2R}, .. E_{mR}$ встановлюється в одиницю.

14. Індекс u поточного біту контрольної послідовності S встановлюється в одиницю.

15. Якщо значення довжини l_{jR} менше за $(h_2 - 2)$, тобто $l_{jR} < h_2 - 2$, то перевіряються умови:

15.1Якщо $l_{jR} \bmod 4 = c_u + 2 \cdot c_{u+1}$, то перехід на п.20.

15.2Якщо $(l_{jR} + 1) \bmod 4 = c_u + 2 \cdot c_{u+1}$, то j-тий фрагмент передано з помилкою синхронізації: приймач зменшив кількість одиниць в j-тому фрагменті на один. Відповідно, фрагмент E_{jR} збільшується на одну одиницю. Перехід на п.20.

15.3Якщо $(l_{jR} - 1) \bmod 4 = c_u + 2 \cdot c_{u+1}$, то фрагмент E_{jR} передано з помилкою синхронізації: приймач збільшив кількість одиниць в j-тому фрагменті на один. Корекція виконується шляхом видалення з фрагменту E_{jR} однієї одиниці. Перехід на п.20.

16. Якщо значення довжини l_{jR} дорівнює $(h_2 - 2)$: $l_{jR} = h_2 - 2$, то виконується перевірка наступних умов:

16.1Якщо $l_{jR} \bmod 4 = c_u + 2 \cdot c_{u+1}$, то перехід на п.20.

16.2Якщо $(l_{jR} + 1) \bmod 4 = c_u + 2 \cdot c_{u+1}$, то фрагмент E_{jR} передано з помилкою синхронізації: зменшення кількості одиниць на стороні приймача в j-тому фрагменті на один. Корекція відбувається шляхом додавання одиниці до фрагменту E_{jR}. Перехід на п.20.

16.3Якщо $(l_{jR} - 1) \bmod 4 = c_u + 2 \cdot c_{u+1}$, то фрагмент E_{jR} передано з помилкою синхронізації: збільшення кількості одиниць на стороні приймача в j-тому фрагменті на один. Відповідно у фрагменті E_{jR} вида-ляється одиниця. Перехід на п.20.

16.4Якщо $(l_{jR} + 2) \bmod 8 = c_u + 2 \cdot c_{u+1} + 4 \cdot c_{u+2}$, то фрагмент E_{jR} передано з помилкою синхронізації: зменшення кількості одиниць в j-тому фрагменті на два на приймачі. Для корекції фрагмента E_{jR} потрібно додати дві одиниці. Перехід на п.21.

17. Якщо значення довжини l_{jR} дорівнює $(h_2 - 1)$: $l_{jR} = h_2 - 1$, то перевіряються наступні умови:

17.1Якщо $l_{jR} \bmod 4 = c_u + 2 \cdot c_u + 1$, то перехід на п.20.

17.2Якщо $(l_{jR} - 1) \bmod 4 = c_u + 2 \cdot c_u + 1$, то фрагмент E_{jR} передано з помилкою синхронізації: збільшення кількості одиниць на стороні приймача в j-тому фрагменті на один. Корекція реалізується шляхом видалення одиниці у фрагменті EjR. Перехід на п.20.

17.3Якщо $(l_{jR} + 1) \bmod 8 = c_u + 2 \cdot c_u + 1 + 4 \cdot c_u + 2$, то при передачі j-того фрагмента виникла помилка синхронізації: приймач зменшив кількість одиниць в j-тому фрагменті на один. Відповідно до фрагмента E_{jR} додається одиниця. Перехід на п.21.

17.4Якщо $(l_{jR} + 2) \bmod 8 = c_u + 2 \cdot c_u + 1 + 4 \cdot c_u + 2$, то j-тий фрагмент передано з помилкою синхронізації: приймач зменшив кількість одиниць в j-тому фрагменті на два. Відповідно до фрагмента E_{jR} додаються дві одиниці. Перехід на п.21.

18. Якщо значення довжини l_{jR} дорівнює h_2: $l_{jR} = h_2$, то перевіряються наступні умови:

18.1Якщо $(u + 1) = q$, то фрагмент E_{jR} містить помилку синхронізації альтернативного типу: збільшення кількості одиниць на стороні приймача в j-тому фрагменті на один. Для корекції фрагмента E_{jR} вида-ляється одиниця. Перехід на п.20.

18.2Якщо $l_{jR} \bmod 8 = c_u + 2 \cdot c_{u+1} + 4 \cdot c_{u+2}$, то перехід на п.21.

18.3Якщо $(l_{jR} + 1) \bmod 8 = c_u + 2 \cdot c_{u+1} + 4 \cdot c_{u+2}$, то фрагмент E_{jR} передано з помилкою синхронізації: приймач зменшив кількість одиниць в j-тому фрагменті на один. Відповідно до фрагмента E_{jR} додається одиниця. Перехід на п.21.

18.4Якщо $(l_{jR} - 1) \bmod 4 = c_u + 2 \cdot c_{u+1}$, то фрагмент E_{jR} передано з помилкою синхронізації: збільшення кількості одиниць на стороні приймача в j-тому фрагменті на один. Для корекції фрагмента E_{jR} вида-ляється одиниця. Перехід на п.20.

18.5Якщо $(l_{jR} + 2) \bmod 8 = c_u + 2 \cdot c_{u+1} + 4 \cdot c_{u+2}$, то j-тий фрагмент передано з помилкою синхронізації: приймач зменшив кількість одиниць в фрагменті E_{jR} на два. Корекція відбувається шляхом додавання двох одиниць до фрагмента E_{jR}. Перехід на п.21.

19. Якщо значення довжини l_{jR} більше h_2: $l_{jR} > h_2$ то перевіряються наступні умови:

19.1Якщо $(u + 1) = q$, то у j-тому фрагменті при передачі виникла помилка синхронізації: приймач збільшив кількість одиниць в j-тому фрагменті на два. Корекція фрагмента E_{jR} відбувається шляхом вида-лення двох одиниць. Перехід на п.20.

19.2Якщо $l_{jR} \bmod 8 = c_u + 2 \cdot c_{u+1} + 4 \cdot c_{u+2}$, то перехід на п.21.

19.3Якщо $(l_{jR} + 1) \bmod 8 = c_u + 2 \cdot c_{u+1} + 4 \cdot c_{u+2}$, то фрагмент E_{jR} містить помилку синхронізації: зменшення кількості одиниць на стороні приймача в j-тому фрагменті на один. Відповідно до фрагмента E_{jR} дода-ється одиниця. Перехід на п.21.

19.4Якщо $(l_{jR} - 1) \bmod 8 = c_u + 2 \cdot c_{u+1} + 4 \cdot c_{u+2}$, то фрагмент E_{jR} передано з помилкою синхронізації: приймач збільшив кількість одиниць в j-тому фрагменті на один. Корекція фрагмента E_{jR} відбувається шляхом видалення одиниці. Перехід на п.21.

19.5 Якщо $(l_{jR} + 2) \bmod 8 = c_u + 2 \cdot c_{u+1} + 4 \cdot c_{u+2}$, то j-тий фрагмент передано з помилкою синхронізації: зменшення кіль-кості одиниць на стороні приймача в фрагменті E_{jR} на два. Для корекції фрагмента E_{jR} відбувається додавання двох одиниць. Перехід на п.21.

19.6 Якщо $(l_{jR} - 2) \bmod 8 = c_u + 2 \cdot c_{u+1} + 4 \cdot c_{u+2}$, то фрагмент E_{jR} передано з помилкою синхронізації: збільшення кількості одиниць на стороні приймача в j-тому фрагменті на два. Відповідно у фрагменті E_{jR} видаляються дві одиниці. Перехід на п.21.

19.7 Якщо $(l_{jR} - 2) \bmod 4 = c_u + 2 \cdot c_{u+1}$, то j-тий фрагмент передано з помилкою синхронізації: на приймачі в j-тому фрагменті виникло два додаткових одинич-них біта. Корекція фрагмента E_{jR} відбу-вається шляхом видалення двох одиниць. Перехід на п.20.

20. Індекс u збільшується на два: $u = u + 2$. Перехід на п.22.

21. Індекс u збільшується на три: $u = u + 3$.

22. Якщо $j < m$, то виконується інкремент значення лічильника: $j = j + 1$ та повернення на п. 15.

23. Кінець.

Запропонований метод може бути проілюстрований наступним прикладом:

Припустимо, що критичні межі h_1 та h_2 існування ризику виникнення одно і дво-кратних помилок синхронізації дорівнюють h_1=4 та h_2=8. Це означає, що: для послідовності E одиниць, довжина l якої менша або дорівнює h_1: $l \le h_1$ виникнення помилок синхронізації практично неможливе; для послідовності E одиниць, довжина l якої лежить в межах $h_1 + 1 \le l < h_2$, не може виникнути більше однієї помилки: тобто довжина послідовності на приймачеві може змінитися не більш ніж на одиницю; для послідовності E одиниць, довжина l якої більша або дорівнює h_2: $l \ge h_2$ може виникнути одна або дві помилки синхронізації: тобто довжина фрагменту E не може змінитися більш ніж на два біти.

Нехай, з передавача надсилається 64-бітовий блок B_S = {0**111 11**01 0001 0**111 1111 1**001 0**111 1**010 1000 **1111 1111 1**010 0001 0**111 1111** 0101}. Згідно з запропонованим методом, у блоці B_S виділяються послідовності одиничних бітів, кількість яких не менша h_1. Блок B_S містить 5 (m = 5) таких послідовностей E_{1S}, E_{2S}, …, E_{5S}, що виділені жирним шрифтом. Кількість одиниць у фрагментах відповідно становить: $l_{1S} = 5$, $l_{2S} = 8$, $l_{3S} = 4$, $l_{4S} = 9$, $l_{5S} = 7$.

Лічильник j виділених фрагментів встанов-люється в одиницю: $j = 1$.

Індекс u поточного біта контрольної послідовності S встановлюється в одиницю: u=1.

Оскільки довжина l_{1S} першого фрагмента дорівнює 5: $l_{1S} \in [h_1; h_2)$, то обчислюються два біти $<c_1, c_2>$ контрольної послідовності S, шляхом отримання залишку від ділення довжини l_{1S} на чотири: $c_1 + 2 \cdot c_2 = l_{1S} \bmod 4 = 5 \bmod 4 = 01$. Індекс u збільшується на два: $u = u + 2 = 1 + 2 = 3$. Згідно п.9 умова $j < m$ виконується:1<5, отже, значення лічильника інкрементується: $j = 2$.

Так як довжини l_{2S} другого фрагмента дорівнює h_2: $l_{2S} = 8$, то формуються наступні три біти $<c_3, c_4, c_5>$ контрольної послідовності S, що обчислюються як залишок від ділення довжини l_{2S} на вісім: $c_3 + 2 \cdot c_4 + 4 \cdot c_5 = l_{2S} \bmod 8 = 8 \bmod 8 = 000$. Індекс u збільшується на три: $u = u + 3 = 3 + 3 = 6$. Оскільки значення лічильника j менше, ніж кількість фрагментів m, виконується збільшення лічильника на один: $j = 3$.

Довжина l_{3S} третього фрагмента дорівнює h_1: $l_{3S} = 4$, тому виконується обчислення наступних двох бітів $<c_6, c_7>$ контрольної послідовності S. Визначається залишок від ділення довжини l_{3S} на чотири: $c_6 + 2 \cdot c_7 = l_{3S} \bmod 4 = 4 \bmod 4 = 00$. Згідно п.7 збільшується індекс u на два: $u = u + 2 = 6 + 2 = 8$. Відповідно до п.9 виконується умова $j < m$ (3 < 5), тому інкрементується значення лічильника: $j = 4$.

Оскільки довжина l_{4S} четвертого фрагмента дорівнює 9: $l_{4S} \in [h_2; \infty)$, то обчислюються наступні три біти $<c_8, c_9, c_{10}>$ контрольної послідовності S, котрі визна-чаються як залишок від ділення довжини l_{4S} на вісім: $c_8 + 2 \cdot c_9 + 4 \cdot c_{10} = l_{4S} \bmod 8 = 9 \bmod 8 = 001$. Відповідно до п.7 збільшується індекс u на три: $u = u+3 = 8+3 = 11$. Значення лічильника j менше, ніж кількість фрагментів m: 4 < 5, змінна j збільшується на один: $j = 5$.

Довжина l_{5S} п'ятого фрагмента дорівнює 7: $l_{5S} \in [h_1; h_2)$, то обчислюються два біти $<c_{11}, c_{12}>$ контрольної послідовності S, шляхом отримання залишку від ділення довжини l_{5S} на чотири: $c_{11} + 2 \cdot c_{12} = l_{5S} \bmod 4 = 7 \bmod 4 = 11$. Індекс u збільшується на два: $u = u + 2 = 11 + 2 = 13$. Оскільки значення лічильника j дорівнює кількості фрагментів m, то процес формування контрольної послідовності S завершено. Отже, контрольна послідовність S складається з таких бітів: S = {0100 0000 0111}.

Приймач отримує помилковий блок даних B_R = {0**111** **1**010 0010 **1111** **11**00 10**11** **111**0 1010 00**11** **1111** **1111** 0100 0010 **1111** **1111** 0101}. У блоці B_R виокремлюються фрагменти E_{1R}, E_{2R}, …, E_{5R}, що містять послідовність одиниць, кількість яких не менша h_1. Прийнятий блок B_R має 5 ($m = 5$) потрібних послідовностей E_{1R}, E_{2R}, …, E_{5R}, які виділені жирним шрифтом. Довжини цих фрагментів відповідно дорівнюють: $l_{1R} = 4$, $l_{2R} = 6$, $l_{3R} = 5$, $l_{4R} = 10$, $l_{5R} = 8$.

Лічильник j помилкових фрагментів встановлюється в одиницю: $j = 1$.

Індекс u поточного біта контрольної послідовності S встановлюється в одиницю: u=1.

Оскільки $l_{1R} < h_2 - 2$ (4 < 6), то аналізуються умови з пунктів 15.1 – 15.3 для визначення факту помилки в поточному фрагменті чи його відсутності. Перевіряється умова $l_{1R} \bmod 4 = c_1 + 2 \cdot c_2$, оскільки умова не справджується – $l_{1R} \bmod 4 \neq 01$ (4 mod 4 ≠ 01, 00 ≠ 01) – приймається рішення про отримання фрагмента E_{1R} з помилкою синхронізації. Для визначення типу помилки перевіряється умова $(l_{1R} + 1) \bmod 4 = c_1 + 2 \cdot c_2$, яка в даному випадку виконується – (4 + 1) mod 4 = 01 (01 = 01). Відповідно до п.15.2 фрагмент E_{1R} прийнятий з помилкою: зменшення на стороні приймача кількості одиниць у фрагменті. Корекція помилки здійс-нюється шляхом додавання одиничного біта до фрагмента E_{1R}. Згідно п.20 індекс u збільшується на два: $u = u + 2 = 1 + 2 = 3$. Оскільки значення лічильника j менше, ніж кількість фрагментів m, виконується збіль-шення лічильника на один: $j = 2$.

Так як довжина l_{2R} другого фрагмента дорівнює $h_2 - 2$: $l_{2R} = 6$, то виконується аналіз умов з пунктів 16.1 – 16.4. Згідно п. 16.1 здійснюється перевірка умови $l_{2R} \bmod 4 = c_3 + 2 \cdot c_4$, яка в даному випадку не виконується: 6 mod 4 ≠ 00 (10 ≠ 00), що свідчить про наявність помилки у фрагменті E_{2R}. Відповідно до п.16.2 здійснюється перевірка умови $(l_{2R} + 1) \bmod 4 = c_3 + 2 \cdot c_4$ – рівність не виконується: (6 + 1) mod 4 ≠ 00 (11 ≠ 00). Перевіряється умова $(l_{2R} - 1) \bmod 4 = c_3 + 2 \cdot c_4$, що також не виконується: (6 – 1) mod 4 ≠ 00 (01 ≠ 00). Згідно п.16.4 аналізується умова $(l_{2R} + 2) \bmod 8 = c_3 + 2 \cdot c_4 + 4 \cdot c_5$ – рівність справджується: (6 + 2) mod 8 ≠ 000 (000 ≠

000). Приймається рішення про наявність помилки синхронізації: приймач зменшив кількість одиниць у фрагменті E_{2R} на два. Корекція такої помилки виконується шляхом додавання двох одиниць до фрагмента E_{2R}. Відповідно п.21 індекс u збільшується на три: $u = u + 3 = 3+3 = 6$. Згідно п.22 виконується умова $j < m$ (2 < 5), тому інкрементується значення лічильника: j=3.

Оскільки $l_{3R} < h_2 - 2$ (5 < 6), тому проводиться аналіз умов з пунктів 15.1 – 15.3. Виконується перевірка умови $l_{3R} \bmod 4 = c_6 + 2 \cdot c_7$ – умова не підтверджується: 5 mod 4 ≠ 00 (5 mod 4 ≠ 00, 01 ≠ 00), що свідчить про наявність помилки синхронізації в фрагменті E_{3R}. Перевіряється умова $(l_{3R} + 1) \bmod 4 = c_6 + 2 \cdot c_7$, яка не виконується: (5 + 1) mod 4 ≠ 00 (6 mod 4 ≠ 00, 10 ≠ 00). Згідно з п.15.3 перевіряється рівність $(l_{3R} - 1) \bmod 4 = c_6 + 2 \cdot c_7$, яка виконується: (5 – 1) mod 4 = 00 (4 mod 4 ≠ 00, 00 ≠ 00). Відповідно помилкою є поява додаткового одиничного біта у фрагменті E_{3R} при передачі. Виконується корекція в третьому фрагменті прийнятого блоку B_R: видаляється один несинхронізований біт. Індекс u збільшується на два: $u = u + 2 = 6 + 2 = 8$. Значення лічильника j менше, ніж кількість фрагментів m: 3 < 5, змінна j збільшується на один: $j = 4$.

Оскільки $l_{4R} > h_2$ (10 > 8), то аналізуються умови з пунктів 19.1 – 19.7. У силу того, що умова $(u + 1) = 12$ не виконується: – 10 ≠ 12, то відбувається перехід до наступного пункту. Перевіряється умова $l_{4R} \bmod 8 = c_8 + 2 \cdot c_9 + 4 \cdot c_{10}$, так як рівність не виконується: $l_{4R} \bmod 8 \neq 001$ (10 mod 8 ≠ 001, 010 ≠ 001) – четвертий фрагмент прийнятий з помилкою синхронізації. Відповідно до п.19.2 рівність $(l_{4R} + 1) \bmod 8 = c_8 + 2 \cdot c_9 + 4 \cdot c_{10}$ не справджується: $l_{4R} \bmod 8 \neq 001$ (11 mod 8 ≠ 001, 011 ≠ 001). Тому перевіряється умова з п.19.3 $(l_{4R} - 1) \bmod 8 = c_8 + 2 \cdot c_9 + 4 \cdot c_{10}$, що в даному випадку виконується: $l_{4R} \bmod 8 = 001$ (9 mod 8 = 001, 001 = 001). Таку помилку класифікують як помилку синхронізації альтер-нативного типу: приймач збільшив кількість одиниць в четвертому фрагменті на один. Для корекції виявленої помилки виконується вилу-чення одиниці з фрагмента E_{4R} прийнятого блоку. Індекс u збільшується на три: $u = u + 3 = 8 + 3 = 11$. Оскільки значення лічильника j менше, ніж кількість фрагментів m, вико-нується збільшення лічильника на один: $j = 5$.

Так як довжина l_{5R} п’ятого фрагмента прийнятого блоку дорівнює 8: $l_{5R} = h_2$, то проводиться аналіз умов з пунктів 18.1 – 18.5. У силу того, що умова $(u + 1) = 12$ виконується: тобто – (11 + 1 = 12), це означає наявність помилки синхронізації: збільшення на стороні приймача кількості несинхронізованих одиниць у фрагменті. Корекція помилки виконується шляхом видалення одиничного біта з фрагмента E_{5R}.

Оскільки значення лічильника j дорівнює кількості фрагментів m, то процес корекції помилок завершено.

Для розглянутого прикладу виявлено, що переданий блок B_R містить п'ять помилок синхронізації в п'яти фрагментах: у фрагменті E_{1R} зник одиничний біт, у фрагменті E_{2R} зникло два одиничних біта, у фрагменті E_{3R} з’явився додатковий одничний біт, у фрагменті E_{4R} виник один одиничний біт та у фрагменті E_{5R} з’явився додатковий одничний біт.

Скоригований інформаційний блок на приймачі має вигляд: B_R = {0**111 11**01 0001 0**111 1111 1**001 0**111 1**010 1000 **1111 1111 1**010 0001 0**111 1111** 0101} та відповідає надісланому передавачем блоку B_S.

4. Аналіз ефективності

Основна перевага розробленого методу корекції помилок синхронізації, у порівнянні з існуючими полягає у тому, що він дозволяє виправляти більш широкий клас помилок. У порівнянні з відомими методами позитивною відмінністю запропонованого є відсутність обмежень на кількість помилок, що можуть бути виправлені: метод дозволяє коригувати помилки синхронізації, що можуть виникнути при передачі всіх, потенційно небезпечних послідовностей бітів, передача яких не синхронізована.

На відміну від всіх існуючих, запропо-нований метод базується на розширеній моделі виникнення помилок синхронізації. Всі існуючі методи виходять з моделі того, що при передачі послідовності несихронізованих бітів може виникнути максимум одна помилка. Це означає, що згадані методи не здатні виправляти дві помилки, що потенційно

можуть виникнути при передачі довгих послідовностей несин-хронізованих бітів.

У розширеній моделі виникнення помилок синхронізації передбачається для коротких послідовностей (довжиною не більшою ніж h_1) можливість виникнення однієї помилки, а для більш довгих послідовностей – розширена модель передбачає можливість виникнення двох помилок синхронізації. Відповідно, розроблений метод, що базується на цій моделі, забезпечує можливість виправлення двох помилок, що потенційно можуть виникнути при передачі довгих послідовностей несинхронізованих бітів.

Важливою перевагою запропонованого методу є можливість гнучкого налаштування параметрів методу у відповідності до характеристик реального каналу передачі даних. Цей факт є особливо важливим для систем управління об'єктами та процесами в реальному часі, компоненти яких працюють у різних температурних режимах. Зокрема, мова йде про комп'ютерні системи управління літальними апаратами, в яких число цифрових датчиків може сягати до 250 тис. До класу згаданих систем відносяться також цифрові комплекси управління об'єктами та технологічними проце-сами, пов'язаними з термообробкою.

Зокрема, параметри розробленого методу гнучко налаштовуються в залежності від фактичної кількості виникаючих помилок: при збільшенні числа помилок значення критичної межі h зменшується та навпаки. Також можливе гнучке налаштування в процесі роботи каналу в залежності від типу каналу або від різниці температур приймача та передавача (напри-клад, для літаків значення критичної межі h на землі становить: h = 6, а на висоті – h = 3-4).

Число контрольних k символів, які додатково передаються разом з інформаційним блоком являє собою випадкову величину, що залежна від його довжини n.

Припускаючи, що нульові та одиничні біти в n-бітовому блоці даних зустрічаються з рівною ймовірністю, нескладно показати, що середня кількість фрагментів, що складаються рівно з j одиниць дорівнює $n / 2^{j+2}$. Відповідно, середня кількість k_1 фрагментів інформаційного блоку, що складаються зі слідуючих підряд від $h_1 - 1$ до $h_2 - 1$ бітів, передача яких несинхронізована визначається як сума:

$$k_1 \approx \sum_{j=h_1-1}^{h_2-1} \frac{n}{2^{j+2}} \approx \frac{n}{2^{h_1}} \cdot (1 - \frac{1}{2^{h_2-h_1}}) \quad (3)$$

Середня кількість k_2 фрагментів інформаційного блоку, що складаються зі слідуючих підряд не менш ніж h_2 несинхронізованих бітів визначається як сума:

$$k_2 \approx \sum_{j=h_2}^{\infty} \frac{n}{2^{j+2}} \approx \frac{n}{2^{h_2}} \quad (4)$$

Оскільки для кожної послідовності довжиною від $h_1 - 1$до $h_2 - 1$ несинхронізованих при передачі бітів в запропонованому методі використовується два контрольних біти, а для послідовностей більшої довжини – 3 біти, то загальна середня кількість k контрольних розрядів визначається формулою:

$$k = 2 \cdot k_1 + 3 \cdot k_2 \approx \frac{n}{2^{h_1-1}} \cdot (1 - \frac{1}{2^{h_2-h_1}}) + \frac{3 \cdot n}{2^{h_2}} \quad (5)$$

Наприклад, якщо при типовому значенні h_1=4, h_2=8 контролюється передача блоку довжиною 256 байт (n = 2048), то згідно (5), середня кількість контрольних розрядів k становить: k = 264. Відповідно, запропонований метод передбачає додаткову передачу k = 264 бітової контрольної послідовності, що ста-новить 12.89% від довжини блоку.

Відомий метод, що здатен коригували помилки синхронізації при передачі всіх послідовностей несинхронізованих бітів, за умови, що для кожної такої послідовності може бути втрачено або додано лише один біт, використовують за цих умов 256 контрольних розрядів, тобто має рівень надлишковості, практично аналогічний запропонованому ме-тоду. Використання бітового стаффінгу потребує передачі додаткового біту для кожної з послідовності довжиною більше h_1-1 одиниць, тобто 2^{11-4} = 128 додаткових бітів. Таким чином, запропонований метод, має високі функціональні можливості щодо виправлення помилок синхронізації і при цьому за рівнем надлишковості практично мало відрізняється від відомих методів.

5. Висновки

У результаті проведених досліджень розроблено метод виправлення помилок синхронізації, відмінністю якого є можливість корекції вказаного класу помилок за умови втрати чи додавання більш ніж одного біту в процесі передачі довгих послідовностей бітів, передача яких не синхронізована. Це дозволило роз-ширити клас помилок синхронізації, що можуть бути виправлені в порівнянні з відомими методами.

Запропонований метод дозволяє гнучко змінювати параметри процедур корекції в залежності від реальних характеристик виникаючих помилок синхронізації і, цим самим, забезпечує можливість автоматичного підлаштування коригуючої здатності безпосередньо під час передачі при зміні характеру виникаючих помилок. Це дозволяє ефективно реалізувати корекцію виникаючих помилок передачі даних в системах комп'ютерного управління літальними апаратами та технологічними процесами.

Список літератури

1. Klove T. Error Detecting Codes: General Theory and Their Application in Feedback Communication Systems / T. Klove, V. Korzhik - Norwell, MA: Kluwer, 1995. – 433 p.

2. Fedorechko O., Markovskyi O.P., Doukas N., Bardis N. Synchronization Error Detection of Data Transmission Errors in Asynchronous Channels // Recent Advances in Electrical Engineering Series - 37. Latest trends on Systems.- Vol.1.- Proceeding of the 18-th International Conference on Systems - CSCC-14. - Santorini Island, Greece, July 17-21. 2014. - ISSN: 1790-5117, ISBN: 978-1-61804-243-9. P.179-183.

УДК 004.75

МАРТИНЮК Р.О.
ЛУЦЬКИЙ Г.М.
ВОЛОКИТА А.М.
РОТЕНБЕРГ О.В.

СПОСІБ РОЗПОДІЛЕНИХ ОБЧИСЛЕНЬ З ВИКОРИСТАННЯМ WEB БРАУЗЕРІВ

В даній роботі описано використання WEBбраузерів для створення системи розподілених обчислень на основі технологій JavaScript та AJAX. Описане рішення має дві основні переваги: воно не потребує встановлення додаткових програм для обчислення, працюючи у фоновому режимі, тим самим не заважаючи клієнту.

This article is describes how to use WEB browsers to create a system of distributed computing through technology JavaScript and AJAX. The described solution has two main advantages: it does not require additional software to calculate and working in the background without disturbing a client.

Ключові слова :розподілені обчислення, web-браузер, клієнт-серверна архітектура.

1. Вступ

Розподілені обчислення – це спосіб, який використовують для розв'язання задач, котрі можливо розділити на декілька частин, названих підзадачами; кожна з них вирішується окремо, зазвичай за допомогою незалежних комп'ютерів або процесорів. Після завершення обчислень збираються результати, щоб сформувати остаточне рішення первинної задачі.

Більшість проектів, на основі розподілених обчислень, були розроблені протягом останніх років. Це, наприклад, проект Folding@home Хімічного факультету Стенфордського університету, або SETI@home Лабораторії Космічних досліджень Каліфорнійського університету Берклі, також серед таких проектів LHC@home [1].

Загальний аспект проектів, описаних вище, це використання клієнт серверної архітектури, для якої необхідно встановлювати додаткове ПО на комп'ютер користувача (клієнта).

Робота, яка описана в даній статі, презентує розробку системи розподілених обчислень на основі клієнт-серверної архітектури, яка використовує велику кількість клієнтів, з'єднаних через мережу Інтернет. Основною інновацією системи є ідея реалізації розподілених обчислень без встановлення будь-якого додаткового ПО на стороні клієнта, а з використанням лише прямих можливостей web-браузера. Ми використовуємо клієнтський web-браузер для того, щоб виконувати обчислення під час роботи користувача. Код, який описує реалізацію підзадачі на стороні клієнта, вбудований у web-сторінку завдяки технологіям AJAX та JavaScript. При кожному відвідуванні сайту, користувачі будуть виконувати певні розрахунки у фоновому режимі[1]. На даний момент web-браузери не дозволяють напряму контролювати завантаженість системи на стороні клієнта, без встановлення додаткових розширень.

Головна мета цієї роботи – перевірити фактичну реалізацію цього підходу і виміряти можливості архітектури в процесі виконання розподілених обчислень на великій кількості клієнтів.

2. Реалізація архітектури системи

Система розподілених обчислень, яку ми розробили, основана на використанні web-браузера користувачем. Його класичний опис в цьому контексті більш широкий: браузер – це не лише програма для перегляду веб-сторінок, але і інструмент, який має можливість виконувати обчислення задач.

Завдяки технологіям JavaScript та AJAX клієнту не потрібно встановлювати додаткове ПО, так як код, для виконання задач, він буде отримувати з серверу. Таким чином, число потенційних клієнтів набагато більше порівняно з випадком, коли клієнт встановлює спеціальні програми для комунікації з сервером[3].

Під час перегляду сторінки, користувач, завдяки технології AJAX, у фоновому режимі отримує код підзадачі, котра почне виконуватись, і по завершенню відішле результат на сервер. Додаток має збережені на сервері дані та збережену на стороні клієнта логіку, тому важливим етапом є комунікація клієнта з сервером, передача даних.

Сучасні web-браузери пропонують декілька інструментів для зберігання інформації на стороні клієнта. Крім стандартного SessionStorage, ми можемо використовувати WebWorkers, LocalStorage, IndexedDB, WebSQL. Разом це приблизно 50 мб пам'яті, в котрій ми можемо зберігати інформацію для наших обчислень, на стороні клієнта.

Архітектура системи побудована за принципом клієнт-сервер. Клієнти, вбудовані у веб-сторінку, надсилають запити на отримання підзадач, і відправляють результати на сервер. Цей процес повторюється при активному підключенні користувача, у нашому випадку при відвідуванні сайту. На стороні сервера вирішується декілька задач: розділення первинної задачі на підзадачі, отримання результатів від клієнтів, консолідація результатів, формування комплексного рішення та моніторинг статусу підзадач, що враховують відключення клієнтів, та не правильне виконання.

Задачі для клієнта необхідно формувати на мові JavaScript. Використовуючи можливості AJAX та XMLHttpRequest, клієнт звертається до серверу щоб отримати скрипт, в якому міститься код рішення для отриманої підзадачі.

У свою чергу сучасні браузери реалізують підтримку технології WebWorkers, яка дозволяє виконувати код в декількох потоках, тобто виникає можливість паралельного виконання задач на стороні клієнта. Для цього, під час ініціалізації, отримаємо кількість процесорів, і, якщо можливо, розділимо підзадачу на менші частини, котрі будуть оброблювати WebWorkers. Після завершення роботи кожного з них, в головному потоці збираємо результат, опрацьовуємо його, і відправимо на сервер.

У випадку, якщо браузер не підтримує технологію WebWorkers, необхідно контролювати виконання задачі в одному потоці, не використавши весь ресурс процесора, і дати користувачу можливість продовжити роботу, без затримок.

Сторона сервера займається розподіленням задач на підзадачі, комунікацією з клієнтами через http-протокол для передачі та отримання результатів, їх обробку. Логіка сервера розділена на сервіси, з котрими працюють клієнти через GET та POST методи, використовуючи AJAX. Сервіси роблять запити до бази даних для отримання параметрів підзадач та збереження результатів. Статус виконання задач, їх результати, та дані користувачів необхідно зберігати для моніторингу статистики, прогресу, кількості невиконаних підзадач, та рейтингу клієнтів.

3. Приклад реалізації задачі

Задача, для якої була проведена оцінка архітектури:

• Факторизація числа методом Полларда:

Даний ρ-алгоритм не є найефективнішим на даний момент, але його можливо розділити на незалежні субзадачі, що дає можливість запустити його на нашій системі для її оцінки.

Реалізація алгоритму має наступний вигляд:

```
function Pollard (N){
var x = random(1, N-2);
var y = 1; var i = 0; var stage = 2;
  while (NOD, Math.abs(x - y)) == 1){
    if (i == stage ){
      y = x;
      stage = stage*2;
    }
    x = (x*x - 1)%N;
    i = i + 1;
  }
  return NOD (N, abs(x-y));
}
```

Дана функція є однаковою для всіх клієнтів, але початкове число x, генеруємо не випадковим чином, а отримуємо набір з серверу. У такому випадку сервер контролює, щоб згенеровані набори не повторювались для клієнтів.

Уявимо, що є P однакових клієнтів. Якщо ми використовуємо P різних послідовностей F(x), то ймовірність того, що перші kчисел в цих послідовностях будуть різні по модулю p

буде $\exp(-k^2P/2p)$. Таким чином максимальне прискорення можна оцінити як $P^{1/2}$ [4].

У свою чергу підзадача, котру ми отримуємо з сервера, може бути виконана в декілька потоків. На стороні клієнта ми можемо реалізувати це за допомогою технології WebWorkers. Для реалізації необхідно виділити JavaScript файл, з необхідною функцією. Він буде виконуватись у незалежному потоці, і після завершення, результат буде переданий до головного потоку.

Деякі ітерації можуть займати багато часу, і не матимуть можливості бути виконаними за одну сесію користувача. У даному випадку необхідно зберігати статус виконання, та дані на стороні клієнта. Сучасні браузери дають змогу використовувати WebSQL - базу даних, яка може зберігати необхідну для нас інформацію.

Таким чином, клієнт отримує від сервера скрипт з кодом функції, та набір даних. Для кожного потоку буде виділятись даний код, та частина даних. Після виконання всіх потоків, результат буде зібраний, і надісланий на сервер.

4. Метрики та результати

В даному розділі представлені метрики, котрі дають змогу вести оцінку як задачі, так і самої системи. Виділимо наступні характеристики:

D : розмір запиту на отримання та надсилання даних

t_D : час на виконання D запиту

t_{calc} : час виконання підзадачі клієнтом

Завдяки вищезгаданим характеристикам можна визначити деякі метрики для того, щоб оцінити продуктивність системи в різних ситуаціях і вирішити в яких випадках доцільне застосування додатку.

Однією з найголовніших метрик є коефіцієнт ефективності обчислення підзадач на стороні клієнта T_c (2). Якщо коефіцієнт близький до одиниці, або навіть більше його, то застосовувати дану систему для вирішення підзадачі неефективно, так як час передачі інформації більший за час обчислення:

$$T_c = \frac{t_D}{t_{calc}} \quad (2)$$

Даний приклад архітектури обмежується одним сервером, і відповідно всі клієнти, котрих може бути багато тисяч, або мільйонів, ведуть обмін даними з ним в онлайн режимі. Тому необхідно розраховувати навантаження на мережу (3), щоб зменшити час черги на отримання даних. Для кожної задачі необхідно ввести параметр обрахунку кількості пакетів даних, до часу виконання задачі D_s. Якщо складність задач не є лінійною, і чим більше даних, тим більший час виконання, то ймовірно, збільшення кількості переданих вхідних даних, може збільшити коефіцієнт, що зменшить навантаження на мережу, але збільшить час виконання підзадачі на стороні клієнта, і відповідно зменшить ймовірність її виконання.

$$D_s = \frac{D}{t_{calc}} \quad (3)$$

При розподіленні задачі на підзадачі важливою характеристикою є час(4), за який головна задача повинна бути виконана, так званий T_d - дедлайн реального часу. Позначимо кількість підзадач як N. Таким чином можемо вивести залежність, як:

$$T_d = (t_D + t_{calc}) * N \quad (4)$$

Дана залежність є ідеальною, адже тут не враховується кількість відмов, і час виконання підзадачі для всіх клієнтів рівний. В реальних умовах, кожен клієнт має свою продуктивність, і час виконання може бути різний. В такому випадку необхідно ввести певний коефіцієнт k_d, який буде змінювати час (5), виданий на обчислення. Також необхідно оновлювати статус підзадач, котрі були отримані клієнтами, але не виконані. Необхідно ввести певний максимальний час виконання T_m, після проходження якого підзадача повертається у статус невиконаної.

$$T_m = (t_D + t_{calc}) * k_d \quad (5)$$

Індекс T_c вказує на відношення між часом передачі даних та часом обчислення задачі. Чим вище коефіцієнт, тим гірше система підходить для вирішення задачі. Адже час передачі даних перевищує час виконання підзадач.

Нарешті коефіцієнт D_s показує використання даних отриманих клієнтом: оптимальне значення наближене до 0. В алгоритм факторизації Пірсона значення, даної характеристики, близькою до мінімальної, адже вхідні дані мають малий розмір, а час на їх обрахунок порівняно великий. Таким чином, даний індекс дає загальне уявлення про продуктивність і не є надто важливим при порівнянні для різних задач, але дає уявлення про використання даних, і можливу оптимізацію розміру задач.

5. Висновок

В даній роботі був запропонований модифікований спосіб розподілених обчислень з використанням web браузерів, що дасть змогу, теоретично, отримати багатомільйонну групу клієнтів, кількість яких з кожним роком зростає. Це спричинене мінімальними затратами при підключенні користувача до системи. Необхідно лише відкрити web сторінку у своєму браузері. Даний спосіб дає змогу виконувати підзадачі в декілька потоках, завдяки технології WebWorkers, що дозволяє у фоновому режимі виконувати обчислення, не заважаючи користувачу продовжувати свою роботу в web браузері.

Для достовірності обрахунків необхідно ввести певний рейтинг оцінки користувачів. Підзадачі виконуються на стороні клієнта, і це дає змогу змінити результати обчислень, і надіслати недостовірну інформацію на сервер. Для цього необхідно вести рейтинг користувачів, перевіряючи їхні обчислення на інших клієнтах. Це збільшить час виконання головної задачі, за рахунок повторних однакових обчислень, але забезпечить достовірність результатів.

Інша проблема – це втрата результатів обчислень, у випадку коли клієнт отримав підзадачу, але результат не був надісланий. Необхідно виділити середній час, і у випадку, коли ми не отримаємо результат за цей час, вважати задачу не виконаною, і віддати цю підзадачу іншому клієнту. Даний підхід збільшить кількість повторного виконання, але результат буде більш достовірний.

Система розподілених обчислень, описана в даній статі може бути використана для благодійних обчислень, так як її використання для комерційних цілей не раціональна.

Список літератури

1. Boldrin F., Taddia C., Mazzini G. Distributed computing through web browser //Vehicular Technology Conference, 2007. VTC-2007 Fall. 2007 IEEE 66th. – IEEE, 2007. – С. 2020-2024.

2. Заикин О. С., Семёнов А. А., Посыпкин М. А. Процедуры построения декомпозиционных множеств для распределенного решения SAT-задач в проекте добровольных вычислений SAT@ home //Управление большими системами: сборник трудов. – 2013. – №. 43.

3. Templin C., Templin J., Shearer A. Encryption system using web browsers and untrusted web servers : пат. 9537864 США. – 2017.

4. Pollard, J. Theorems on factorization and primality testing. Mathematical Proceedings of the Cambridge Philosophical Society, 76(3), 521-528. doi:10.1017/S0305004100049252.

УДК 004.75

ОВЧАРЕНКО П.О.,
ПОДРУБАЙЛО О.О.

АНАЛІЗ МЕТОДУ ГОРИЗОНТАЛЬНОГО МАСШТАБУВАННЯ СИСТЕМ ТА ЙОГО ОСНОВНІ ОСОБЛИВОСТІ

У даній статті розглянуто види масштабувань додатків, а також особливості побудови розподілених масштабованих додатків та основні проблеми, що виникають при їх розробці.

The subject of the article is an application scaling types and features of scalable distributed applications and basic problems that arise in their design.

6. Вступ

У час швидкого розвитку IT технологій, розростання додатків, та ресурсів для їх підтримки виникає проблема, коли один сервер вже не може впоратись з покладеною роботою. Основними функціями серверів є відповідь на HTTP-запити, але, якщо даних для обробки або самих запитів забагато, один сервер може відмовити, зупинивши роботу всього додатку, для того, щоб уникнути таких ситуацій, розробники використовують масштабованість.

Масштабованість - це властивість обчислювальної системи, що забезпечує передбачуваний ріст системних характеристик, наприклад, числа підтримуваних користувачів, швидкості реакції, загальної продуктивності та іншого, при додаванні до неї обчислювальних ресурсів . Наприклад сервера СУБД можна розглядати два способи масштабування - вертикальний і горизонтальний

Вертикальне масштабування - це збільшення потужності окремого сервера СУБД і досягається заміною апаратного забезпечення (процесор, диски) на більш швидкодіючі або додаванням додаткових вузлів. Хорошим прикладом може служити збільшення числа процесорів в симетричних багатопроцесорних (SMP) платформах. При цьому програмне забезпечення сервера не повинно змінюватися

При горизонтальному масштабуванні системи з'єднуються через мережу або об'єднуються в кластер. Для міжз'єднань зазвичай використовуються стандартні мережеві технології, такі, як Fast Ethernet, Gigabit Ethernet (GBE) і Scalable Coherent Interconnect (SCI), що дають меншу пропускну здатність і більше запізнювання в порівнянні з вертикальними системами. Ресурси в цьому випадку розподіляються між вузлами, зазвичай містять від одного до чотирьох процесорів; кожен вузол має власний процесор і пам'ять і може мати власну підсистему введення-виведення або використовувати її спільно з іншими вузлами. На кожному вузлі працює окрема копія ОС. Ресурси розширюються за рахунок додавання вузлів, але не додавання ресурсів в вузол. Пам'ять в горизонтальних системах розподілена, тобто у кожного

вузла є власна пам'ять, до якої безпосередньо звертаються його процесори і підсистема вводу-виводу. Доступ до цих ресурсів з іншого вузла відбувається набагато повільніше, ніж з вузла, де вони розташовані. Крім того, при горизонтальній архітектурі відсутній узгоджений доступ вузлів до пам'яті, а використовувані додатки споживають відносно небагато ресурсів, тому вони "поміщаються" на одному вузлі і їм не потрібен узгоджений доступ. Якщо ж з додатком буде потрібно кілька вузлів, то воно саме повинно забезпечити узгоджений доступ до пам'яті.[1]

Якщо горизонтальна система задовольняє вимогам додатків, то така архітектура краща, оскільки витрати на її

придбання менше. Зазвичай вартість придбання в розрахунку на один процесор у горизонтальних систем нижче, ніж у вертикальних. Різниця в ціні пояснюється тим, що в вертикальних системах застосовуються більш потужні функції надійності, доступності та обслуговування - RAS (reliability, availability, serviceability), а також високопродуктивні міжз'єднання. Однак є ряд обмежень на застосування систем з горизонтальною архітектурою. Інший спосіб горизонтального масштабування - це великі обчислювальні системи з масовим паралелізмом (MPP), що складаються з безлічі встановлених в одній шафі невеликих процесорів, кожен з яких має власну копію ОС або копію мікроядра ОС. В даний час випускаються всього кілька систем MPP, які найчастіше представляють спеціалізовані рішення. Це, наприклад, системи Terradata виробництва компанії NCR, IBM RS / 6000SP (SP-2) і HP Tandem non-stop.[2]

Таблиця1. Типи додатків для вертикальної и горизонтальної архітектури

Вертикальні системи	Горизонтальні системи
•Великі бази даних •Бази даних транзакцій •Сховища даних •Поглиблене вилучення даних •Сервери додатків • Програми НРТС (не розбиваються на розділи)	• Web-сервери • Брандмауери • Проксі-сервери • Робота з потоковим мультимедіа • Каталоги • Обробка XML • Програми JSP • Шифрування SSL • Віртуальні приватні мережі (VPN) • Сервери додатків • Програми НРТС (розбиваються на розділи)

2. Особливості побудови масштабованого розподіленого додатку

При побудові розподіленого масштабованого додатку потрібно враховувати наступні особливості:

2.1 Сесії

Необхідно відстежувати навігацію користувачів по сайту. Для вирішення цього завдання зазвичай використовується механізм сесій, який полягає в привласненні кожному відвідувачу унікального ідентифікаційного номера, який йому передається для зберігання в cookies, або, в разі їх відсутності, для постійного "тягання" за собою через GET. Отримавши від користувача деякий ID разом з черговим HTTP-запитом сервер може подивитися в список вже виданих номерів і однозначно визначити хто його відправив. З кожним ID може асоціюватися якийсь набір даних, який веб-додаток може використовувати на свій розсуд, ці дані зазвичай за замовчуванням зберігаються в файлі в тимчасовій директорії на сервері.

Запити відвідувачів одного і того ж сайту можуть обробляти відразу кілька серверів, в такому випадку для визначення який саме сервер видав ID використовують наступні рішення:

- Централізоване зберігання сесій

Ідея проста: створюється для всіх серверів загальну "скарбничку", куди вони зможуть складати видані ними сесії і

дізнаватися про сесії відвідувачів інших серверів. У ролі такої "скарбнички" теоретично може виступати і просто примонтована по мережі файлова система, але більш перспективним виглядає використання будь-якої СУБД, так як це позбавляє від маси проблем, пов'язаних зі зберіганням сесійних даних в файлах. Але в варіанті із загальною базою даних не варто забувати, що навантаження на нього буде неухильно зростати зі зростанням кількості відвідувачів, а також варто заздалегідь передбачити варіанти виходу з проблематичних ситуацій, пов'язаних з потенційними збоями в роботі сервера з цією СУБД.

- Децентралізоване зберігання сесій

Наочний приклад - зберігання сесій в memcached, спочатку розрахована на розподілене зберігання даних в оперативній пам'яті система дозволить отримувати всім серверам швидкий доступ до будь-яких сесійних даних, але при цьому (на відміну від попереднього способу) будь-який єдиний центр їх зберігання буде відсутній. Це дозволить уникнути вузьких місць з точок зору продуктивності і стабільності в періоди підвищених навантажень.

В якості альтернативи сесіям іноді використовують схожі за призначенням механізми, побудовані на cookies.

2.2 Статичний контент

Поки обсяги статичних даних невеликі - ніхто не заважає зберігати їх в локальній файловій системі і надавати доступ до них просто через окремий легкий веб-сервер, але рано чи пізно ліміт сервера по дисковому простору або файловій системі за кількістю файлів в одній директорії буде досягнутий, і потрібно перерозподілити дані. Тимчасовим рішенням може стати розподіл даних по їх типу на різні сервера, або, можливо, використання ієрархічної структури каталогів.

Якщо статичний контент відіграє одну з основних ролей в роботі додатка, то варто задуматися про застосування розподіленої файлової системи для його зберігання. Це, мабуть, один з небагатьох способів горизонтально масштабувати обсяг дискового простору шляхом додавання додаткових серверів без будь-яких кардинальних змін в роботі самого додатка.

Альтернативою цьому підходу виступає використання так званих Content Delievery Network - зовнішніх сервісів, що забезпечують доступність Вашого контенту користувачам за певну матеріальну винагороду сервісу. Перевага очевидна - немає необхідності організовувати власну інфраструктуру для вирішення цього завдання, але зате з'являється інша додаткова стаття витрат.

2.3 Кешування

Кешування є сенс проводити на всіх етапах обробки даних, але в різних типах додатків найбільш ефективними є лише деякі методи кешування.

- СУБД

Практично всі сучасні СУБД забезпечують вбудовані механізми для кешування результатів запитів. Цей метод досить ефективний, якщо Ваша система регулярно робить одні й ті ж вибірки даних, але також має ряд недоліків, основними з яких є інвалідація кеша всієї таблиці при найменшій її зміні, а також локальне розташування кешу, що неефективно при наявності декількох серверів в системі зберігання даних.

- Додаток

На рівні додатків зазвичай проводиться кешування об'єктів будь-якої мови програмування. Цей метод дозволяє зовсім уникнути значної частини запитів до СУБД, сильно знижуючи навантаження на неї. Як і самі додатки такий кеш повинен бути незалежний від конкретного запиту і сервера, на якому він виконується, тобто бути доступним всім серверам додатків одночасно, а ще краще - бути розподіленим по декільком машинам для більш ефективної утилізації оперативної пам'яті. Лідером в цьому аспекті кешування по праву можна назвати Memcached — комп'ютерна програма, сервіс кешування даних в оперативній пам'яті на основі парадигми розподіленої хеш-таблиці.

- HTTP-сервер

Багато веб-серверів мають модулі для кешування як статичного контенту, так і результатів роботи скриптів. Якщо сторінка рідко оновлюється, то використання цього методу дозволяє без будь-яких видимих для користувача змін уникати генерації сторінки у відповідь на досить велику частину запитів.

- Reverse proxy

Поставивши між користувачем і веб-сервером прозорий проксі-сервер, можна видавати користувачу дані з кешу проксі (який може бути як в оперативній пам'яті, так і дисковим), не доводячи запити навіть до HTTP-серверів. У більшості випадків цей підхід актуальний тільки для статичного контенту, в основному різних форм медіа-даних: зображень, відео тощо. Це дозволяє веб-серверам зосередитися тільки на роботі з самими сторінками.

Кешування за своєю суттю практично не вимагає додаткових витрат на обладнання, особливо якщо уважно спостерігати за використанням оперативної пам'яті іншими компонентами сервера і утилізувати всі доступні "надлишки" під найбільш підходящі форми кеша.[4]

2.4 База даних

База даних є важливим компонентом веб застосування, яке складно масштабувати. Як вирішення цієї проблеми використовують заміну майстер сервера на master-slave з асинхронною реплікацією даних при такому підході всі операції запису виконуються лише на одному сервері (master), а інші сервера (slave) отримують дані безпосередньо від "майстра", обробляючи при цьому лише запити на читання даних. Як відомо, операції читання і запису будь-якого веб-проекту завжди ростуть пропорційно зростанню навантаження, при цьому зберігається майже фіксованим співвідношення між обома типами запитів: на кожен запит на оновлення даних зазвичай доводиться в середньому близько десятка запитів на читання. Згодом навантаження зростає, а значить зростає і кількість операцій запису в одиницю часу. Рано чи пізно витрати операцій реплікації даних стануть настільки високі, що цей процес стане займати дуже велику частину процесорного часу кожного сервера, а кожен slave зможе обробляти лише порівняно невелика кількість операцій читання, і, як наслідок, кожен додатковий slave-сервер почне збільшувати сумарну продуктивність лише незначно, теж займаючись здебільшого лише підтриманням своїх даних відповідно до "майстра".

Тимчасовим вирішенням цієї проблеми може стати заміна master-сервера на більш продуктивний, але так чи інакше не вийде нескінченно відкладати перехід на наступний "рівень" розвитку системи зберігання даних: «sharding». Ідея полягає в тому, щоб розділити всі дані на частини по будь-якою ознакою і зберігати кожну частину на окремому сервері або кластері, таку частину даних в сукупності з системою зберігання даних, в якій вона знаходиться , і називають сегментом або shard'ом. Такий підхід дозволяє уникнути витрат, пов'язаних з реплікацією даних (або скоротити їх у багато разів), а значить і істотно збільшити загальну продуктивність системи зберігання даних. Але, на жаль, перехід до цієї схеми організації даних вимагає масу витрат іншого роду. Так як готового рішення для її реалізації не існує, доводиться модифікувати логіку додатку або додавати додатковий "прошарок" між додатком і СУБД, причому все це найчастіше реалізується силами розробників проекту. Готові продукти здатні лише полегшити їх роботу, надавши якийсь каркас для побудови основної архітектури системи зберігання даних і її взаємодії з іншими компонентами програми.

На такій стадії база даних може горизонтально масштабуватися для забезпечення вимог найважчих систем.

- Денормалізація

Запити, що комбінують дані з декількох таблиць, зазвичай при інших рівних вимагають більшого процесорного часу для виконання, ніж запит, який стосується лише однієї таблиці.

- Логічне розбиття даних

Якщо якась частина даних завжди використовується окремо від основної маси, то іноді має сенс виділити її в окрему незалежну систему зберігання даних.

- Низькорівнева оптимізація запитів

Ведучи і аналізуючи логи запитів, можна визначити найбільш повільні з них. Заміна знайдених запитів на більш ефективні з тією ж функціональністю може допомогти більш раціонально використовувати обчислювальні потужності.[4]

Варто згадати ще один, більш специфічний, тип інтернет-проектів. Такі проекти оперують даними, що не мають чітко формалізовану структуру, в таких ситуаціях використання реляційних СУБД в якості сховища даних, м'яко кажучи, недоцільно. У цих випадках зазвичай використовують бази даних з більш примітивною функціональністю в плані обробки даних, але зате вони здатні обробляти величезні обсяги інформації не чіпляючись до її якості та відповідності формату. В якості основи для такого сховища даних може служити кластерна файлова система, а для аналізу же даних в такому випадку використовується механізм під назвою MapReduce. Отже, на вході якісь довільні дані і не факт що в правильно дотриманому форматі. В результаті потрібно отримати якесь підсумкове значення або інформацію. Відповідно до даного механізму практично будь-який аналіз даних можна провести в наступні два етапи:

- Map

Основною метою даного етапу є уявлення довільних вхідних даних у вигляді проміжних пар ключ-значення, що мають певний сенс і формально оформлених. Результати піддаються сортуванню і гуртування по ключу, а після чого передаються на наступний етап.

- Reduce

Отримані після map значення використовуються для фінального обчислення необхідних підсумкових даних.

Кожен етап кожного конкретного обчислення реалізується у вигляді незалежного міні-додатки. Такий підхід дозволяє практично необмежено розпаралелювати обчислення на величезній кількості машин, що дозволяє обробляти обсяги практично довільних даних. Для цього достатньо лише запустити ці програми на кожному доступному сервері одночасно, а потім зібрати воєдино всі результати. Прикладом готового каркаса для реалізації роботи з даними за таким принципом служить opensource проект Apache Foundation під назвою Hadoop.[5]

3. Висновок.

Використання горизонтальної масштабованості вимагає від додатку бути розподіленим, а також зробити реалізацію функціонала у відповідності вимог, які виникають при масштабуванні. В результаті отримана система являтиме собою додаток, що реагує на будь-яку кількість запитів, та об’єм оброблюваних даних і горизонтально масштабуватись у потрібний момент, що дозволить економити кошти власників додатку.

Перелік посилань

1. Кузнецов С. Д., Посконин А. В. Распределенные горизонтально масштабируемые решения для управления данными // Труды ИСП РАН. 2013.[Інтернет ресурс]. URL: http://cyberleninka.ru/article/n/raspredelennye-gorizontalno-masshtabiruemye-resheniya-dlya-upravleniya-dannymi .

2. C. Strozzi, «NoSQL: A Relational Database Management System,» [Інтернет ресурс]. URL: http://www.strozzi.it/cgibin/CSA/tw7/I/en_US/nosql/Home%20Page.

3. D. Karger, A. Sherman, A. Berkheimer, B. Bogstad, R. Dhanidina, K. Iwamoto, B. Kim, L. Matkins и Y. Yerushalmi, «Web Caching with Consistent Hashing,» MIT Laboratory for Computer

Science, 1999. [Інтернет ресурс]. URL: http://www8.org/w8-papers/2awebserver/caching/paper2.html.

4. D. Obasanjo, «Building scalable databases: Denormalization, the NoSQL movement and Digg,» 2009. [Інтернет ресурс]. URL: http://www.25hoursaday.com/weblog/2009/09/10/BuildingScalableDatabases DenormalizationTheNoSQLMovementAndDigg.aspx.

5. “MapReduce Tutorial” [Інтернет ресурс]. URL: https://hadoop.apache.org/docs/r1.0.4/mapred_tutorial.html.

УДК 621.372.542

ОВЧАРЕНКО П.О.
САВЕРЧЕНКО В.Г.

ЦИФРОВА ФІЛЬТРАЦІЯ В СИСТЕМАХ ОБРОБКИ ЗОБРАЖЕНЬ

Досліджуються низкочастотна просторова та медіанна фільтрації зображень, спотворених дією імпульсних завад. Особлива увага приділяється модифікованому методу медіанної фільтрації для пошкодженого зображення, який використовує подвійну обробку апертури фільтру. Такий модифікований медіанний фільтр дозволяє суттєво поліпшити якість зображення.

The methods of low-frequency spatial and median filtering of images distorted by the action of impulse noise. Particular attention is paid to the modified median filtering method for the distorted image, which uses a double processing of the filter aperture. Such a modified median filter allows to significantly improve image quality.

1. Вступ

Актуальність вирішення задач обробки зображень загальновідома. Серед них одна із найважливіших є корекція зображень. Корекція зображень – це приведення до необхідних значень характеристик зображень. Одним із прикладів корекції може бути усунення завад [1].

Багато задач вилучення інформації з зображень можуть і повинні вирішуватися автоматичними пристроями. Спотворенні завадами зображення суттєво ускладнюють їх автоматичну обробку. Підвищення якості зображень досягається фільтрацією, що послаблює дію завад. Цифрове зображення уявляє собою двовимірну функцію. Найчастіше корисний сигнал змінюється повільніше, ніж завада. Тому підвищення якості зображень на основі цифрової фільтрації передбачає зміну атрибутів поточних пікселів в залежності від атрибутів пікселів, що їх оточують.

7. Постановка задачі

Найбільше застосування одержали фільтри “ковзного вікна”, що використовують атрибути оточуючих пікселів. На зображенні виділяють вікно розміром $N \times M$ пікселів, де значення N та M непарні числа. Тоді поточний центральний піксель вікна є деякою функцією лише елементів вікна.

Для обробки зображень з метою підвищення їх якості використовують різні процедури фільтрації, що дозволяють вилучати імпульсні завади. Найпростішим прикладом фільтра ковзного вікна є низькочастотний фільтр, коли значення центрального пікселя замінюється в залежності від маски фільтру, обчисленого по всіх пікселях вікна.

При медіанної фільтрації центральний піксель вікна замінюється медіаною всіх пікселів зображення у вікні, тобто пікселем для якого існує половина елементів вікна, менших або рівних йому за величиною, і половина елементів, більших або рівних йому за величиною.

8. Фільтрація зображень

Оскільки шум просторово декорельований, в його спектрі, як правило, містяться вищі просторові частоти, ніж в спектрі звичайного зображення. Отже, проста низькочастотна фільтрація може служити ефективним засобом згладжування шумів. Низькочастотна фільтрація зображення передбачає сканування спотвореного зображення двомірним вікном певного розміру.

Масив відфільтрованого зображення C формується за допомогою дискретної згортки масиву початкового зображення

A з масивом фильтру F, який часто називається шумопослаблюючею маскою.

Низькочастотна фільтрація – це метод лінійної обробки зображень Для такої фільтрації при скануванні апертури зліва направо і зверху вниз обчислення виконуються за формулою:

$$C_{r,s} = \frac{1}{k} \cdot \sum_{i=-1}^{1} \sum_{j=-1}^{1} A_{r+i,s+i} \cdot F_{i+1,j+1}$$

де $C_{r,s}$ – матриця пікселів зображення після фільтрації; $r = \overline{1,n-2}$; $s = \overline{1,m-2}$; n та m – кількість строк та рядків відповідно; $A_{r+i,s+i}$ – значення пікселів матриці початкового зображення з завадами; $k = \sum_{i=0}^{2} \sum_{j=0}^{2} F_{i,j}$ – коефіцієнт нормалізації; F – матриця коефіцієнтів фільтру. Для низькочастотних фільтрів можна навести такі приклади масок:

$$F1 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix};$$

$$F2 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 1 \end{pmatrix};$$

$$F3 = \begin{pmatrix} 1 & 2 & 1 \\ 2 & 4 & 2 \\ 1 & 2 & 1 \end{pmatrix}.$$

Маска $F1$ являє собою усереднену фільтрацію, для якої коефіцієнт нормалізації $k = 9$.

Використання коефіцієнта нормалізації дозволяє отримати одиничний коефіцієнт передачі, щоб процедура фільтрації шуму не викликала зміщення середньої яскравості обробленого зображення.

На основі використання таких фільтрів можуть бути розроблені інші процедури фільтрації. Наприклад, процедура порогового фільтру, обчислює пікселі наступним чином. Якщо яскравість пікселя x перевищує середню яскравість групи q_i найближчих пікселів на деяку порогову величину, то яскравість пікселя змінюється на середню яскравість. Наприклад, для вікна 3×3 пікселя $\begin{pmatrix} q_1 & q_2 & q_3 \\ q_4 & x & q_5 \\ q_6 & q_7 & q_8 \end{pmatrix}$, якщо $\left[x - \frac{1}{8} \cdot \sum_{i=1}^{8} q_i \right] \geq \varepsilon$, то $x = \frac{1}{8} \cdot \sum_{i=1}^{8} q_i$.

Метод підвищення контрасту з використанням оператора Лапласа може використовувати такі маски:

$$L1 = \begin{pmatrix} 0 & -1 & 0 \\ -1 & 4 & -1 \\ 0 & -1 & 0 \end{pmatrix};$$

$$L2 = \begin{pmatrix} -1 & -1 & -1 \\ -1 & 8 & -1 \\ -1 & -1 & -1 \end{pmatrix};$$

$$L3 = \begin{pmatrix} 1 & -2 & 1 \\ -2 & 4 & -2 \\ 1 & -2 & 1 \end{pmatrix}.$$

Медіанна фільтрація – це метод нелінійної обробки сигналів. Одновимірний медіанний фільтр являє собою ковзне вікно, яке охоплює непарне число пікселів зображення. Центральний елемент замінюється медіаною всіх елементів зображення у вікні. Медіаною дискретної послідовності $a_1, a_2, \ldots, a_n$ для непарного n є той її елемент, для якого існує $\frac{n-1}{2}$ елементів, менших або рівних йому за величиною, і $\frac{n-1}{2}$ елементів, більших або рівних йому за величиною.

Концепцію медіанного фільтру легко узагальнити на два виміри, застосовуючи двовимірне вікно бажаної форми, наприклад, прямокутне або близьке до

кругового. Очевидно, що двовимірний медіанний фільтр з вікном розміру $n \times n$ забезпечує більш ефективне усунення завад, ніж послідовно застосовані горизонтальний і вертикальний одномірні медіанний фільтри вікном розміру $n \times 1$.

Медіанний фільтр більш ефективно послаблює імпульсні завади, ніж гладкі шуми.

Процедура медіанної фільтрації на мові MathCad має вигляд:

```
A := READBMP("image.bmp")
i := 0..2          j := 0..2
n := rows(A)       m := cols(A)
r := 0..n − 3      s := 0..m − 3
F_{i,j} := A_{r+i,s+j}
Fun(A,r,s) := | for i ∈ 0..2
              |   for j ∈ 0..2
              |     F_{i,j} ← A_{r+i,s+j}
              | Q ← sort(stack(F^⟨0⟩, F^⟨1⟩, F^⟨2⟩))
              | Q_4
C_{r,s} := Fun(A,r,s)
WRITEBMP("image2.bmp") := C
```

Розглянемо використання вікна розміром 3×3 на прикладі використання усередненої і звичайної медіанної фільтрації. Рис. 1 показує фрагмент початкового зображення з завадами (три середніх пікселя, якого зі значенням 4, являють собою приклад імпульсної завади). На рис. 2 та рис. 3 наведено результат застосування процедури усередненої і звичайної медіанної фільтрацій відповідно.

8	7	6	5	5	5	1
8	7	5	5	1	0	0
7	5	5	0	0	0	0
7	5	0	**4**	**4**	0	0

Рис.1. Зображення

8	7	6	5	5	5	1
8	6	5	4	2	1	0
7	5	4	3	2	1	0
7	5	3	**2**	**1**	1	0

Рис.2. Усереднена фільтрація

8	7	6	5	5	5	1
8	7	5	5	1	0	0
7	5	5	4	0	0	0
7	5	4	**0**	**0**	0	0

Рис.3. Звичайна медіанна фільтрація

Як видно з рис.2 та рис.3 результати фільтрації суттєво відрізняються. Звичайна медіанна фільтрації дає суттєво кращі результати ніж усереднена фільтрація. Медіанна фільтрація дозволяє зменшити кількість завад та більшою мірою зберегти палітру зображення . Але процедура звичайної медіанної фільтрації не забезпечують потрібної якості обробки зображень.

Використання модифікованої медіанної фільтрації зображень, яка передбачає двоетапну обробку кожного пікселя, підвищує якість зображень [3].

Сутність модифікованого способу медіанної фільтрації апертурою $k \times k$ пікселів зображення з координатами x, y полягає в тому, що попередньо виконується фільтрація всіх пікселів, що входять до апертури, центром якої вказано піксель з фіксацією результатів в

окремому допоміжному масиві, після чого виконується фільтрація пікселя $a_{x,y}$ зображення з координатами x, y з урахуванням попередньої фільтрації оточуючих пікселів, що входять в апертуру.

Процедура такої фільтрації пікселя зображення з координатами x, y може бути описана наступним чином:

1. Для всіх пікселів зображення з координатами x+i та y+j (i,j∈{-k,k}, i,j≠0), що входять до поточної апертури, виконується формування допоміжного масиву:

$$b_{i,j} = \frac{a_{x+l,y+q}}{\sum\limits_{\substack{l=-k,..,k,\\ q=-k,..,k}} N(a_{x+i,y+j}, a_{x+l,y+q})} = \frac{k^2-1}{2},$$

де функція N(i,j,c) визначається наступним чином: N(d,c)=1, якщо c > d і N(d,c)=0, якщо c ≤ d.

2. Обчислюється відфільтроване значення пікселя $a^1_{x,y}$ за рахунок заміни попереднього його значення на медіану апертури з допоміжного масиву b:

$$a^1_{x,y} = \frac{b_{l,q}}{\sum\limits_{\substack{l=-k,..,k,\\ q=-k,..,k}} N(a_{x,y}, b_{l,q})} = \frac{k^2-1}{2}.$$

Результат модифікованої медіанної фільтрації має вигляд (рис. 4).

8 7 6 5 5 5 0

8 7 5 5 5 0 0

7 5 5 0 0 0 0

7 5 0 **0 0** 0 0

Рис.4. Модифікована медіанна фільтрація

Таким чином, модифікована медіанна фільтрація повністю усунула завади.

9. Висновки

Звичайний медіанний фільтр практично повністю усунув завади, в той час як усереднений фільтр розмазав завади по зображенню. Звичайний медіанний фільтр пригнічує імпульсні завади, тривалість яких становить менше половини ширини вікна.

Модифікована медіанна фільтрація додаткового підвищує якість фільтрації за рахунок двоетапної обробки кожного пікселя.

Перелік посилань

1. Бузовский О.В., Болдак А.А., Мохаммед Руми М.Х. Компьютерная обработка изображений. – К.: “Корнійчук”, 2001. – 180 с.

2. Гонсалес Р. Цифровая обработка изображений / Р. Гонсалес, Р. Вудс; пер. с англ. В.В. Харитонова.- М.:Техносфера, 2005. – 1072 с.

3. Марковський О.П., Невдащенко М.В., Білашевська А.М. Захищена реалізація фільтрації зображень в grid-системах. // Вісник НТУУ “КПІ”. Інформатика, управління та обчислювальна техніка: збірник наукових праць – К.: “Век+”, 2014. – № 61. – С. 103–109.

УДК 004.052.42

ОЛІЄВСЬКИЙ А.А.

ОРГАНІЗАЦІЯ ЗАХИСТУ ВІД РЕКОНСТРУКЦІЇ ОПЕРАНДІВ МОДУЛЯРНОГО ЕКСПОНЕНЦІЮВАННЯ АНАЛІЗОМ ДИНАМІКИ СПОЖИВАННЯ ПОТУЖНОСТІ

Ціль представлених досліджень полягає в аналізі небезпеки реконструкції операндів модулярного експоненціювання шляхом аналізу динаміки споживання потужності і розробки засобів протидії. Показано, що ступінь модулярного експоненціювання, що являє собою ключем криптографічних алгоритмів RSA, El-Gamal, DSA може бути реконструйована часовим аналізом споживання потужності. В якості протидії розроблено організацію виконання модулярного експоненціювання з використанням маскування. Використання запропонованого алгоритму передбачає використання передобчислень.

The goal of presented by article research is to point out the potential vulnerabilities of modular exponentiation operands reconstruction by power dynamic analysis and to elaborate countermeasures. It has been shown that exponent of modular exponentiation which is secret key of RSA, El-Gamal and DSA can be reconstruction by timing power analysis. For countermeasure the special organization of modular exponentiation by using masking has been worked out. Proposed algorithms using the result of precomputations.

Ключові слова: аналіз динаміки споживання потужності, смарт-карти, криптографічні алгоритми, модулярне експоненціювання, протоколи захисту даних, термінальні обчислювальні пристрої.

1. Вступ

Багато сучасних локальних та розподілених комп'ютерних та телекомунікаційних систем мають розвинуті засоби захисту від сторонніх чи зловмисних впливів на радіоелектронну апаратуру, зокрема, з боку спеціальних криптоаналітичних засобів: це системи управління технологічними процесами в атомній та іншій енергетичній промисловості, системи державного управління, електронних платежів, адміністрування комп'ютерною безпекою та інші. Розробка та дослідження ефективних та високо надійних засобів захисту інформації, які відповідають сучасним стандартам та вимогам до швидкодії, контрольованості та захищеності від несанкціонованого втручання, є однією з провідних проблем в галузі створення комп'ютерні системи та їх компонентів.

Подальший розвиток засобів безпеки в комп'ютерних системах пов'язаний з підвищенням „криптостійкості" як програмних засобів, так і технічних засобів шифрування на мікроелементній базі, які повинні забезпечити не тільки ефективну протидію спеціальним впливам на апаратуру, але і враховувати можливості швидкої модифікації зловмисних впливів.

Разом з проблемою створення стійких до впливів термінальних компонентів систем управління та обчислювальної техніки, стає все більш актуальною науково-технічна проблема адаптації засобів захисту комп'ютерних систем та мереж до модифікацій зловмисних впливів на апаратуру. З'являються все нові фундаментальні наукові роботи в галузі математичних методів аналізу зловмисної активності на вузлах мереж та створення розподілених систем виявлення вторгнень.

Хоча методи та засоби протидії крипто-аналітичним атакам на електронну апаратуру вже мають достатньо розвинуті теоретичну та практичну бази, дослідження та розробка адаптивних та стійких до впливів термінальних компонентів шифрування та захисту телекомунікаційних систем та мереж від зловживань і вторгнень на сучасній

алгоритмічній та технологічній базі є перспективними і актуальними.

До теперішнього часу створені розвинені технології реконструкції значень кодів окремих операндів за результатами вимірювання та аналізу динаміки споживання потужності мікроконтролерами в процесі реалізації ними алгоритмів захисту інформації. Аналіз цих технологій дозволяє зробити висновок про те, що витрати на порушення захисту при використанні динаміки зміни параметрів технічної реалізації при виконанні функцій захисту суттєво нижчі в порівнянні з методами, в основі яких лежить математичний та статистичний аналіз масивів вхідних та вихідних даних роботи криптографічного алгоритму (диференційний і лінійний криптоаналіз). Це створює серйозну небезпеку для надійної реалізації захисту інформації при роботі портативних обчислювальних пристроїв в комп'ютерних мережах и вимагає розробки ефективних засобів протидії.

Таким чином, проблема підвищення стійкості мікроелектронних пристроїв асиметричного шифрування до атак спеціального виду за рахунок внесення додаткових апаратних та структурних компонентів, що підвищує обчислювальну складність проведення атак на термінальні компоненти в системах телекомунікації, диспетчеризації та керування є актуальної і важливою для практики.

2. Аналіз обчислювальних процедур асиметричної криптографії

В основі сучасних алгоритмів асиметричної криптографії лежать мультиплікативні операції модулярної арифметики і, зокрема, модулярного експоненціювання над числами, довжина яких значно перевищує розрядність процесорів.

Традиційно, модулярне експоненціювання $A=X^E \bmod M$ n-розрядних чисел $A, X, M, E=\{e_n e_{n-1}\dots e_1\}$ виконується за n циклів, в кожному i-тому ($i\in\{0,1\}$) з яких оброблюється (починаючи з молодших) i-тий розряд e_i експоненти E: обчислюються значення двох проміжних змінних S_i та A_i, причому $S_i= S_{i-1}\cdot S_{i-1} \bmod M$ і, при $e_i=1$, виконується множення $A_i=A_{i-1}\cdot S_{i-1} \bmod M$. SPA дозволяє визначити факт виконання операції $A_i=A_{i-1}\cdot S_{i-1} \bmod M$ і таким чином визначити значення e_i. Так можна визначити всі n розрядів коду E. Одним з шляхів протидії реконструкції E шляхом аналізу споживання потужності є виконання множення $A_i=A_{i-1}\cdot S_{i-1} \bmod M$ не в своєму, i-тому, циклі. Операція $A_i=A_{i-1}\cdot S_{i-1} \bmod M$ може бути виконана в j-тому циклі ($j>i$) за умови, що в пам'яті будуть збережені значення S_l : $\forall l\in\{i-1,\dots,j-1\}: e_{l+1}=1$.

Значну частину термінальних компонентів комп'ютерних систем і мереж складають портативні обчислювальні пристрої - мікроконтролери та смарт-карти, особливістю яких є те, що в кожний момент часу в них виконується лише один процес, тобто об'єктивно існує зв'язок між даними, що оброблюються і потужністю, яку споживає обчислювальний пристрій.

Сила струму, що споживається портативним обчислювальним пристроєм в момент виконання команди, залежить от типу команди і від кодів операндів та результату. Для портативних обчислювальних пристроїв відносно просто виконати вимірювання динаміки споживання потужності під час виконання програми і поставити у відповідність командам, що виконуються.

На сьогоднішній день існує дві технології такої реконструкції: простий аналіз споживання потужності (SPA -Simple Power Analysis) та диференційний аналіз споживання потужності (DPA - Differentional Power Analysis).

Сутність першої полягає у відновленні за осцилограмою споживання потужності послідовності команд, що виконуються програмою. На рис.1 наведено реальну осцилограму споживання потужності мікроконтролером при виконанні 2-го та 3-го циклів алгоритму DES. Стрілками позначені значення потужності, що співвідносяться з командами зсуву лівої та правої частин ключа. Чітко видно, що на 2-му циклі зсув виконується один раз, а 3-му - два рази.

Ефективність SPA в плані реконструкції даних визначається залежністю порядку виконання програми від цих даних. Наприклад, в основі алгоритмів несиметричного шифрування, цифрового підпису та ідентифікації віддалених абонентів лежить операція модулярного експоненціювання: $A^E \bmod M$ n-розрядних чисел. Процедура обчислення

полягає в виконанні *n* циклів, в кожному з яких реалізується операція піднесення до квадрату і, залежно від поточного біту експоненти - *E* множення на A. Зафіксувавши номери циклів, на яких виконується операція множення достатньо просто реконструювати двійковий код *E*, яка в згаданих вище алгоритмах являє собою секретний код.

Технологія DPA полягає у встановлені статичних залежностей між розрядами даних та потужністю, що споживається обчислювальним пристроєм під час виконання кожної з команд. Тобто ця технологія попереднього статистичного дослідження впливу розрядів даних на споживання потужності в кожний момент часу за умови, що програма не змінюється. Сам процес реконструкції даних за допомогою виявлених залежностей також являє собою статистичний аналіз. Відповідно, такий процес може бути ефективним лише за умови незмінності даних. Існує ряд модифікацій і різновидів технології DPA.

Активне використання технологій SPA і DPA ініціює розробку апаратних та програмних засобів протидії. Застосування апаратних засобів ускладнює структуру портативних обчислювальних компонент та помітно збільшує їх вартість. Тому на практиці більшого розповсюдження набули програмні засоби протидії SPA та DPA. Основними критеріями ефективності таких засобів є рівень захисту, що забезпечується їх застосуванням та об'єм додаткових обчислювальних ресурсів, потрібних для їх реалізації.

Для протидії DPA - технології, що має за основу статистичний аналіз, найбільш ефективними є методи, що базуються на введенні випадковості.

До цієї групи методів протидії відносяться:

- маскування значень даних, що використовуються при кожному виконанні програми (ключів криптографічних алгоритмів) випадковими кодами, які змінюються при кожному запуску програми. Маскування - найбільш простий метод протидії DPA, що потребує найменших додаткових ресурсів для своєї реалізації, хоча існує проблема "зняття маски" для одержання коректного результату. В останні роки з'явилась технологія незаконного доступу до даних - диференційний аналіз споживання потужності (DPA) другого порядку, при використанні якої маскування ключів випадковим кодом не забезпечує їх ефективного захисту від реконструкції.
- стохастичний програмний поліморфізм, що застосовується в двох формах: випадкова вставка команд, що не впливають на результат, але ускладнюють прив'язку моменту виміру потужності до конкретної команди програми; випадкова зміна послідовності виконання незалежних по даним команд.

Найбільш ефективним засобом протидії SPA і DPA є друга форма програмного поліморфізму, тобто випадкова зміна при кожному виконанні програми послідовності виконання команд, яка не впливає на результат. Такий поліморфізм дозволяє ефективно протидіяти DPA високих порядків.

Основним недоліком стохастичного поліморфізму, як засобу протидії SPA і DPA, є значний об'єм обчислювальних ресурсів на його реалізацію. Значною мірою цей недолік зумовлений тим, що в опублікованих дослідженнях задача поліморфної реалізації розв'язується в загальному вигляді, без урахування особливостей конкретного алгоритму. При такій постановці поліморфна реалізація постає доволі складною задачею, розв'язання якої пов'язано з аналізом графу залежності операцій по даним. В ряді публікацій такий аналіз пропонується виконувати динамічно. При такому підході застосування поліморфізму, як засобу протидії незаконній реконструкції ключів криптографічних алгоритмів аналізом споживання потужності, обмежене значним об'ємом потрібних для цього обчислювальних ресурсів, суттєво більшим в порівнянні з іншими методами.

Разом з тим, слід враховувати, що кількість криптографічних алгоритмів, що використовуються в протоколах інформаційного обміну з термінальними компонентами комп'ютерних систем і мереж відносно невелика. Тому обґрунтованою представляється розробка методу ефективної поліморфної реалізації для кожного алгоритму в рамках загальних принципів. Такий підхід

дозволяє повною мірою враховувати структуру алгоритму, особливості його обчислювальних процедур, надає можливість проводити цілеспрямовані еквівалентні його перетворення і отримати в результаті ефективну реалізацію програмного поліморфізму, сумірну за витратами обчислювальних ресурсів з іншими методами.

3. Організація маскування операндів модулярної експоненти

Для досягнення поставленої мети пропонується спосіб виконання модулярного експоненціювання з використанням маскування коду експоненти.

Маскування секретного коду експоненти пропонується здійснювати таким порядком. Вибирається довільне число, що менше за модуль R<M та обчислюється його мультиплікативна інверсія V: $(R \cdot V) \bmod M=1$.

Процедуру маскування експоненти при виконанні модулярного експоненціювання $X^E \bmod M$ пропонується виконувати в наступній послідовності:

1. Перед експоненціюванням обчислюється код $Y=\mathbf{X} \cdot R \bmod M$;
2. Виконується модулярне експоненціювання $G = Y^E \bmod M$
3. Виконується модулярне експоненціювання $Q = V^E \bmod M$
4. Остаточний результат обчислюється у наступному вигляді: $G \cdot Q \bmod M$.

Очевидно, що для запропонованої організації модулярного експонентціювання час виконання збільшується приблизно вдвоє. Проте цей час може бути суттєвим чином зменшено за рахунок використання переобчислень.

Пункт 3 може бути здійснений в рамках передобчисель зі збереженням результату в спеціальній табличній пам'яті. Такі передобчислення виконуються один раз зі збереженням в табличній пам'яті множини пар значень <R,Q>. При кожному виконанні операції модулярного експоненціювання випадковим чином вибирається з табличної пам'яті передобчислень пара значень <R,Q>. За рахунок цього, час виконання модулярного експоненціювання практично не збільшується порівняно зі звичайним обчисленням $X^E \bmod M$ за класичним алгоритмом.

Запропонований спосіб маскування коду експоненти може бути ілюстрований наступним прикладом виконання модулярного експонентами над числами малої розрядності. Нехай обчислюється $5^{11} \bmod 13$. Легко перевірити, що результат дорівнює 8. Відповідно, для цього прикладу X=5, E=11 та M=13. Нехай, згідно наведеної вище процедури, для маскування вибрано значення маски R=7. Його мультиплікативна інверсія дорівнює 2: V=2, оскільки $7 \cdot 2 \bmod 13=1$. Відповідно, в табличній пам'яті зберігається значення $Q= 2^{11} \bmod 13 = 7$. Тоді в рамках п.1 пропонованої процедури обчислюється $Y=5 \cdot 7 \bmod 13 = 9$. Над отриманим значенням у відповідності з п.2 запропонованої процедури здійснюється операція модулярного експоненціювання $G=9^{11} \bmod 13 = 3$. Кінцевий результат, згідно п.4. обчислюється у наступному вигляді: $G \cdot Q \bmod M = 3 \cdot 7 \bmod 13 = 8$.

Ще один варіант маскування коду експоненти полягає в тому, що пропонується m-розрядний двійковий код експоненти E={ e_0, e_1, ..., e_{m-1}} випадковим чином розділити на h груп δ_0, δ_1,...,δ_{h-1} суміжних розрядів, що містять відповідно $n_0,n_1,...,n_{h-1}$ двійкових розрядів. Тоді розряди групи δ_0 відповідають числу g_0, розряди групи δ_{h-1} відповідають числу g_{h-1}.

Тоді код експоненти E може бути представленим у вигляді суми: середньому арифметичному коефіцієнтів точок апертури:

$$E = g_0 + g_1 \cdot 2^{n_0} + g_2 \cdot 2^{n_0+n_1} + ... + g_{h-1} \cdot 2^{m-n_{h-1}} = \sum_{l=0}^{h-1} g_l \cdot 2^{\sum_{j=0}^{l-1} n_j} \quad (1)$$

Якщо ввести позначення w_0=1, $w_1 = 2^{n_0}$,..., $w_{h-1} = 2^{n_0+n_1+n_2+..+n_{h-2}}$, то $A^E \bmod M$ можна представити у вигляді добутку:

$$A^E \bmod M = (\prod_{l=0}^{h-1} (A^{g_l} \bmod M)^{w_l} \bmod M) \bmod M$$

Виходячи з викладеного, пропонується наступний порядок обчислення модулярної експоненти $A^E \bmod M$.

1. Користувач обчислює $R_0 = A^{g_0} \bmod M$, $R_1 = A^{g_1} \bmod M$,..., $R_{h-1} = A^{g_{h-1}} \bmod M$.

2. Обчислюються значення $D_1 = R_1^{w_1} \bmod M$,..., $D_{h-1} = R_{h-1}^{w_{h-1}} \bmod M$.

4. Остаточний результат обчислюється у вигляді $A^E \bmod M = (R_0 \cdot \prod_{i=1}^{h-1} D_i \bmod M) \bmod M$.

При використанні часового аналізу динаміки споживання потужності мікропроцесорним пристроєм під час виконання ним модулярного експоненціювання за запропонованою схемою

Запропонований підхід до маскування коду експоненти може бути конкретизований для деяких застосувань, зокрема для захищеної реалізації алгоритму RSA. Для цього алгоритму код модуля являє собою добуток двох простих чисел: $M = p \cdot q$. це дозволяє реалізувати ідею маскування коду експоненти у вигляді адитивної маски, що є добутком випадково обраного числа r на $\phi(M)=(p-1)\cdot(q-1)$. Замаскована такою маскою експонента E' може бути представлена у вигляді: $E' = E + r\cdot\phi(M)$. В силу того, що для будь-якого X справедливим є $X^{r\cdot\phi(M)} \bmod M = 1$, то $X^{E'} \bmod M = X^E \bmod M$. Це означає, що для зняття такої адитивної маски нема потреби в використанні додаткових операцій. Недоліком запропонованого способу є те, що накладання адитивної маски $r\cdot\phi(M)$ на код експоненти суттєвим чином збільшує розрядність n' коди експоненти E'.

Для захисту від спроб реконструкції секретного коду експоненти пропонується наступний варіант маскування. Якщо вважати коди E і M практично незмінними, то завжди можна знайти множину з h можливих масок $\mathfrak{Y}=\{U_1,U_2,...,U_h\}$. Кожна i-та з масок множини $\mathfrak{Y}$ має наступні властивості:

$$\forall X < M : X^{U_i} \bmod M = 1$$

Маски множини $\mathfrak{Y}$ обчислюються попередньо і зберігаються в табличній пам'яті. При реалізації операції модулярного експоненціювання $X^E \bmod M$ пропонується здійснювати наступну послідовність дій:

1. Вибирається випадковим чином маска $U \in \mathfrak{Y}$.
2. Здійснюється адитивне маскування коду експоненти E вибраним кодом маски: $Y=E+U$.
3. Виконується модулярне експоненціювання з обчисленням $C=X^Y \bmod M$. В силу того, що для X справедливо $X^U \bmod M=1$, то $X^{E+U} \bmod M = (X^E \bmod M + X^U \bmod M) \bmod M = X^E \bmod M$.

Запропонований спосіб маскування може бути проілюстрований наступним прикладом. Нехай потрібно обчислити $5^{11} \bmod 13=8$, тобто $X=5$, $E=11$ та $M=13$. Нехай, далі, згідно п.1 запропонованої процедури в якості адитивної маски вибрано значення $U=12$ таке, що $\forall A<M$: $A^{12} \bmod 13 = 1$. В рамках п.2 пропонованої процедури здійснюється адитивне маскування коду експоненти E вибраним кодом маски: $Y=11+12=23$. У відповідності п.3 описаної вище процедури обчислюється $C=5^{23} \bmod M = 8 = 5^{11} \bmod M$.

4. Висновки

В результаті проведених досліджень, направлених на організацію протидії спробам реконструкції за результатами аналізу динаміки зміни споживання потужності операндів модулярного експоненціювання – базової операції більшості криптографічних алгоритмів шляхом запропоновано ряд способів, в основі яких лежить адитивне маскування.

Доведено, що маскування може бути виконане достатньо просто, але має наслідком суттєве зниження швидкодії. З урахуванням специфічних особливостей модулярного експоненціювання в системах захисту інформації розроблені способи захищеного модулярного експоненціювання фактично без втрати швидкодії.

Список літератури

1. Messerges T.S. Power Analysis Attacks of Modular Exponentiation in Smartcards / T.S. Messerges, E.A.Dabbish // Proceeding of 1-th International Workshop "Cryptographic Hardware and Embedded Systems" (CHES-1999), LNCS-1717. Springer-Verlag.- 1999.- P. 145-157.

2. Костенко Ю. В. Метод защищенного модулярного экспоненциро- вания на удаленных компьютерных системах / Ю.В. Костенко, А.П. Марковский, О.В. Русанова // Вісник Націо-

нального технічного університету України “КПІ” Інформатика, управління та обчислювальна техніка. К.: ТОО „ВЕК+”.- № 64.- 2016.- С. 51-54.
3. Зюзя А.А. Способ противодействия реконструкции ключей блоковых алгоритмов защиты информации анализом динамики потребляемой мощности / А.А.Зюзя // Вісник Національного технічного університету України ”КПІ”. Інформатика, управління та обчислювальна техніка. К.,"ВЕК++",- 2009.- № 50.- С.89-96.
4. Марковский А.П. К проблеме защиты операндов модулярного экспоненцирования от их реконструкции анализом динамики потребления мощности / А.П. Марковский, Мухаммад Мефлех Алиса Абабне, А.А. Зюзя, В.М. Гаразд // Вісник Національного технічного університету України ”КПІ”. Інформатика, управління та обчислювальна техніка. К.,"ВЕК++",- 2007.- № 47.- С.22-32.
УДК 004.75

РОТЕНБЕРГ О.В.
ЛУЦЬКИЙ Г.М.
ВОЛОКИТА А.М.
МАРТИНЮК Р.О.

СПОСІБ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ МОНІТОРИНГУ ОБЧИСЛЕНЬ В РОЗПОДІЛЕНИХ СИСТЕМАХ

У даній роботі розглянуто централізовану модель розподілених обчислень. У системі є централізований сервер (так званий менеджер), що розподіляє задачі між вузлами (агентами) для виконання обчислень. В даній роботі розглянуто способи та підходи для мінімізації обчислень на стороні менеджера та підвищення ефективності перевірки результатів обчислень.

In this work was considered centralized model for distributed computing. System has a centralized server (manager), which distributes tasks between nodes (agents) to perform computing. In this work was considered methods and approaches to minimize calculations and to improve efficiency validation of computing.

Ключові слова : розподілені обчислення, централізований сервер, менеджер, агент.

5. Вступ

Сучасні задачі потребують великі обчислювальні потужності. Системи розподілених обчислень, які координують задачі між тисячами чи навіть мільйонами добровільних агентів стають дедалі популярнішими. Прикладами таких систем є SETI@home та Rosetta@home, мета яких проаналізувати величезні обсяги даних в пошуках позаземного життя чи кращого розуміння процесу згортання білка, відповідно. В цих системах кожне додаткове обчислення приносить більше користі.

У даній роботі розглядається впровадження модифікованої кредитної системи, яка нагороджує чи штрафує агента в залежності від результатів та часу обчислень.

2. Модель

Центральний сервер (менеджер), нагороджує агентів за виконану роботу. Основна ціль - зменшити кількість обчислень на стороні менеджера. В системі агенти запитують нові задачі у менеджера, але в певний момент агент може перестати слати запити на нову роботу.

Менеджер нагороджує агента за коректно виконану роботу нагородою *r*. Якщо менеджер з'ясовує, що агент повернув некоректний результат, менеджер накладає на нього штраф *f,* який вираховується з загального рейтингу агента. Як результат, ми бачимо залежність *f/r* - чим вище співвідношення, тим менша ймовірність, що задача буде видана цьому агенту [1].

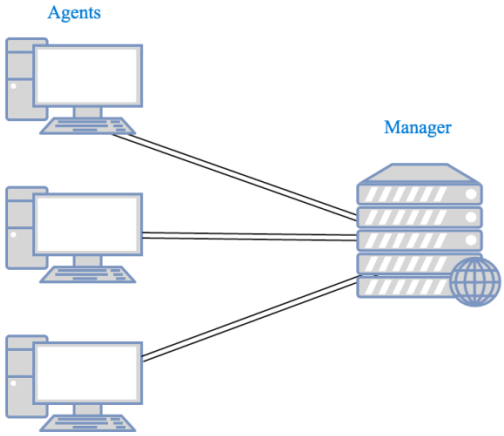

Рис. 1. Централізована модель розподілених обчислень.

Розглянемо випадок, коли менеджер видав задачу агенту. У агента є 2 варіанти. Перший - агент чесно виконає роботу і отримає винагороду r. Якщо ми визначимо вартість обчислень за допомогою алгоритму, що надав менеджер як *cost(i)*, то рентабельність обчислень *u(i)* становитиме $u(i) = r - cost(i)$, де *i* – це і-та задача. В цьому випадку, ми передбачаємо, що r більша від *cost(i)*, інакше агент відмовиться виконувати роботу[1].

У другому випадку агент повертає результат, використовуючи інший алгоритм. Наприклад, агент має уявлення про вигляд відповіді, і намагається її вгадати, чи він має доступ до альтернативного алгоритму, який

надає правильну відповідь з ймовірністю *q* (наприклад оптимізований клієнт SETI@home). У цьому випадку агент все ще може отримати *r*, але великий ризик отримати штраф *f*, якщо менеджер виявить, що результат некоректний.

Позначимо ймовірність того, що менеджер виявив невірну відповідь як *p.* Хоча ми не припускаємо, що менеджер кожен раз в змозі виявити некоректну відповідь та оштрафувати винного агента, оскільки перевірка на коректність може значно збільшити необхідність використання обчислювальних ресурсів менеджера[2]. Якщо менеджер встановлює співвідношення штрафу до инагороди $f/r \geq (1-p)/p$, де $p = c(1-e)$, то раціональний агент поверне коректний результат щонайменше *e* разів, де *c* - ймовірність того, що результат агента буде перевірено [1].

Такий чином, будь який раціональний агент буде використовувати найменш дорогий алгоритм, який забезпечує коректні відповіді щонайменше з ймовірністю *e*.

3. Перевірка результату

Подвійна перевірка

Найбільш простою стратегією для менеджера є випадкова подвійна перевірка отриманої відповіді з ймовірністю *t.* Але менеджер не може знати, чи правильна відповідь, поки її не перевірить, тому *c = t.* Встановлення низького значення *t* надасть можливість менеджеру зменшити кількість роботи пов'язаної з подвійною перевіркою - але так як *c* обернено пропорційне до *f/r*, то високий *f/r* може стати нездоланним бар'єром, для агентів, які шукають роботу[3].

Залучення декількох агентів

Менеджер може мінімізувати кількість перевірок надсилаючи однакову роботу декільком агентам. Менеджер виконує подвійну перевірку лише у випадку, коли у агентів різні результати. Проблема в тому, що якщо всі агенти відправлять одну й ту саму невірну відповідь, то менеджер ніяк не зможе це виявити.

Припустимо, що частка агентів *h* завжди виконують обчислення вірно – автори називають таких агентів «старанними» або «раціональними» [1]. Менеджер обирає *m* агентів випадковим чином і назначає їм одну й ту саму задачу. Опишемо *c* як ймовірність, що агент буде спійманий іншим агентом, якщо він надасть невірну відповідь.

Припустимо, що менеджер надає задачу *m* агентам, кожен з яких виконує задачу чесно з ймовірністю *h,* тоді ймовірність того, що шахрая впіймають, становить $c = 1 - (1-h)^{(m-1)}$ [1].

Ця стратегія все ще потребує від менеджера виконання роботи, коли агенти надсилають різні результати. В системі, де всі агенти раціональні, таких ситуацій взагалі не повинно виникати. Але, якщо існують агенти в змові, чи злодії, вони можуть змусити менеджера виконувати повторну перевірку.

Гібридна стратегія

Менеджер також може застосувати гібридну стратегію : він може надати одну й ту саму задачу декільком агентам та випадковим чином повторно перевірити деякі відповіді. Так, навіть якщо всі агенти в змові нададуть хибну відповідь, менеджер зможе викрити їх.

Залучення 2 раціональних агентів

Менеджер випадковим чином обирає нову групу агентів для кожної задачі. Зробимо припущення, що дані агенти є "сумлінними", і якщо ми коректно встановимо відношення f/r, то основною стратегією для агента буде чесне обчислення.

Тут буде рівність - якщо всі інші агенти обманюють, то і раціональний агент буде також обманювати, і навпаки, якщо хоча б один агент чесний, то і раціональний агент повинен бути чесним.

Ми можемо порушити цю рівність для нечесних агентів, встановивши для них заохочення. Якщо надані різні результати, менеджер перевірить обчислення і нагородить всіх агентів, які надали правильний результат. Тепер очікувана рентабельність за сумлінне виконання задач, коли всі інші вибирають бути лінивими агентами є $u(1) = r - cost(1) + b(1-q)$[1].

Якщо менеджер наймає двох агентів для виконання задачі, тоді він повинен встановити *f/r > 0* і дати чесним агентам $b \geq r/(1-q)$, де b – винагорода, коли вони зловили шахрая [1].

Шкідливі агенти

Шкідливі агенти атакують систему - їх мета знизити точність результатів та збільшити кількість повторних перевірок, які повинен зробити менеджер. Вони не раціональні, але для того, щоб утримуватися в системі, вони повинні тримати хоча б нульовий баланс рентабельності (якщо вони не можуть заплатити штраф, то вони не зможуть бути найняті менеджером) [4]. Шкідливі агенти можуть домовлятися шляхом централізованого контролю, через зовнішні комунікації та навіть через обмін ресурсами (винагорода *r*).

Навіть шкідливий агент повинен підтримувати певний позитивний баланс на своєму рахунку, так як в протилежному випадку менеджер може не надати йому задач для обчислення. Тому, шкідливі агенти, які мають намір відправляти якнайбільше некоректних результатів, повинні також певну частку часу виконувати обчислення коректно.

Модель кредитного скорингу

Якщо рейтинг агента є від'ємним, то для прийняття рішення використовується модель кредитного скорингу. Проблему кредитного скорингу можна розглядати як завдання класифікації: знаючи відповіді на питання анкети x ∈ A, визначити, до якої групи належить позичальник: x ∈ Ag для «хороших клієнтів», і x ∈ Ab для «поганих». При цьому необхідно розуміти, що абсолютно точна класифікація принципово неможлива[6].

Згідно з проведеними дослідженнями [7], до теперішнього часу не отримано відомостей про значні переваги якого-небудь з традиційних методів скорингу в точності одержуваних результатів, тобто рівні похибок при використанні цих методів є порівнянними. Так для одних методів (лінійна регресія) бажано використання рівних часток «поганих» і «хороших», тоді як інші методи (дерева класифікації, байєсовські мережі) вимагають, щоб вибірка відображала реальне співвідношення «поганих» і «хороших» клієнтів. Більшість статистичних методів призводять до побудови правила класифікації, заснованого на лінійній скорингової функції.

При реалізації будемо розглядати 2 методи: регресійний аналіз як один з найпоширеніших методів та лінійне програмування, що дає можливість включити в програму додаткові обмеження. [8,9]

Рівняння множинної регресії (з багатьма змінними) у вигляді:

$$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \cdots + \beta_m X_m + \varepsilon$$

де $X = (X_1, X_2, \dots, X_m)$ - вектор незалежних (пояснюючих) змінних; $\beta = (\beta_1, \beta_2, \dots, \beta_n)$ - вектор параметрів (що визначаються); ε – випадкова помилка (похибка); Y – залежна (пояснювальна) змінна. Для оцінки параметрів β використовується метод найменших квадратів.

В методі лінійного програмування є набір даних, що включає в себе відповіді на питання x_i для кожного з *N* клієнтів і індикатори Y_i. Лінійна функцію *s(x)*, яка розділяє «хороших» і «поганих» клієнтів, шукається з міркувань мінімізації помилки a_i.

$$\begin{cases} a_1 + \cdots + a_N \to min \\ w_1 x_{i1} + \cdots + w_m x_{im} \geq c - a_i, \;\; Y_i = 0, \\ w_1 x_{i1} + \cdots + w_m x_{im} \leq c + a_i, \;\; Y_i = 1, \\ a_i \geq 0 \end{cases}$$

Мінімізація проводиться за змінним $(w_1, \dots, w_n, c, \; a_1, \dots, a_N)$. Додаткові обмеження можна накласти через обмеження відповідних ваг $w_i > w_i^0$.

Модифікований спосіб моніторингу обчислень агентом з часовими обмеженнями

Оптимальний час виконання задачі – це час t_{opt}, за який середньостатистичний агент виконує задачу. Час виконання задачі, це відлік часу від моменту отримання задачі агентом до моменту відправки результату менеджеру. Так як, агенти мають різні обчислювальні потужності, необхідно ввести похибку *del*, яка коригуватиме оптимальний час в залежності від кількості отриманих менеджером результатів конкретної задачі (чим більше відповідей отримано, тим менша *del* відповідно).

При отриманні правильної відповіді, виконаної за оптимальний час t, агент отримує винагороду *rk*, де k – коефіцієнт, значення якого за замовчуванням 1, і при кожній наступній правильній відповіді $k_{new} = k_{old}*(1+del)$, але поки $\frac{f}{rk} > 1$

При отримані правильної відповіді, але за час, що не є оптимальним, агент отримує винагороду *rk*, де *k* – коефіцієнт, значення якого за замовчуванням 1, і при кожній наступній неправильній відповіді k_{new} =

k_{old}*(1- del), але необхідно, щоб cost(rk) була меншою, ніж *rk,* так як при від'ємній рентабельності агенти не матимуть сенсу виконувати задачі.

Стратегія реального часу є додатковим стимулом для чесних агентів. Також, дана стратегія дозволяє менеджеру швидше отримувати результат, та в результаті покращити загальний час обчислення всього обсягу задач [5].

4. Висновки

В даній статті було представлено різні техніки, що можуть бути застосовані для підвищення ефективності розподілених обчислень, перешкоджаючи зайвим обчисленням менеджером або іншими агентами.

В роботі запропоновано модифікований спосіб підвищення ефективності моніторингу обчислень в розподілених системах, який за рахунок використання алгоритмів кредитного скорингу та введення додаткових часових обмежень на виконання обчилювальних задач, дозволяють підвищити рівень коректності обчислень та задавати додаткові характеристики часу виконання задач.

В статті показано використання технік, для визначення розумного *f/r,* при якому всі раціональні агенти поводитимуться чесно, та зменшаться наслідки від зловмисних агентів.

Всі ці техніки необхідні для того, щоб зменшити кількість обчислень, які необхідно виконати менеджеру. Було розглянуто ситуацію, в якій менеджер в змозі платити винагороду і штрафувати агентів.

В подальшій роботі можливі такі модифікації - до моменту, коли виконання роботи розпочалося, агент може надати заставу у вигляді штрафу, який буде стягнуто, у випадку, якщо менеджер розкриє шахрайство. Також, менеджер може надавати різні f/r для різних агентів, пропонуючи більшу винагороду, для тих, хто прийме і умови з більшими штрафами.

Список літератури

1. Belenkiy M. et al. Incentivizing outsourced computation //Proceedings of the 3rd international workshop on Economics of networked systems. – ACM, 2008. – С. 85-90.
2. K. Lai, L. Rasmusson, E. Adar, L. Zhang, and B.A. Huberman. Tycoon: An implementation of a distributed, market-based resource allocation system. Multiagent and Grid Systems, 1(3):169–182, 2005.
3. F. Monrose, P. Wyckoff, and A. Rubin. Distributed execution with remote audit. ISOC NDSS, 1999.
4. P. Golle, and I. Mironov. Uncheatable distributed computations. CT-RSA, 2001.
5. Anderson D. P., Fedak G. The computational and storage potential of volunteer computing //Cluster Computing and the Grid, 2006. CCGRID 06. Sixth IEEE International Symposium on. – IEEE, 2006. – Т. 1. – С. 73-80.
6. ВОЛОКИТА, А. М., et al. Дослідження ефективності приватної хмарної системи для обчислень кредитного скорингу. *Вісник Чернігівського державного технологічного університету. Серія: Технічні науки*, 2013, 4: 115-121.
7. Гараган Сергей Александрович. Метод эмпирической скоринговой функции и его использование в кредитном процессе. // [Електронний ресурс]. Режим доступу: http://crosys.org/empirical_scoring_function.html (дата звернення 15.04.2017) - Назва з екрану.
8. Бородич С.А. Эконометрика. Учебное пособие // Минск: Новое знание, 2001. – 408 с. [Електронний ресурс]. Режим доступу: http://www.economy.bsu.by/library/Бородич_Эконометрика/Бородич_Эконометрика.pdf (дата звернення 10.04.2017) – Назва з екрана.
9. Логистическая регрессия и ROC-анализ - математический аппарат. [Електронний ресурс]. Режим доступу: http://www.basegroup.ru/library/analysis/regression/logistic/ (дата звернення 15.04.2017) – Назва з екрана.

УДК 004.056.5

РУДЕНКО Т.А.

МЕТОД СИНТЕЗУ ОРТОГОНАЛЬНИХ СИСТЕМ БУЛЕВИХ ФУНКЦІЙ, ЩО ЗАДОВОЛЬНЯЮТЬ КРИТЕРІЙ СТРОГО ЛАВИНОВОГО ЕФЕКТУ

Доповідь присвячена проблемі побудови ортогональних систем булевих функцій, що задовольняють критерій строго лавинового ефекту. У статті запропоновано та теоретично обґрунтовано новий метод побудови таких систем булевих функцій. Детально описано алгоритм використання методу. Приклад його використання також наведено у статті.

Доклад посвящен проблеме построения ортогональных систем булевых функций, которые удовлетворяют критерий строго лавинного эффекта. В статье предложен и теоретически обоснован новый метод построения таких систем булевых функций. Детально описан алгоритм применения метода. Пример его использования также приведен в статье.

The presentation deals with problem of designing orthogonal boolean SAC-function systems. A new method of building such function systems is offered and theoretically proved in the article. The detailed algorithm and the example of its usage is also given in the article.

1. Вступ

Системи булевих функцій часто використовуються в якості нелінійного перетворювача для псевдовипадкових двійкових послідовностей, що в сучасних умовах широко застосовуються для захисту інформації під час її передачі в комп'ютерних мережах і телекомунікаційних системах. Для того, щоб забезпечити достатньо високу ефективність захисту, ці функції повинні мати високу нелінійність, а також відповідати критерію лавинового ефекту. У зв'язку з цим виникає задача розробки ефективних методів проектування систем ортогональних нелінійних SAC-функцій.

2. Огляд існуючих рішень

Всі запропоновані до теперішнього часу методи синтезу ортогональних систем SAC-функцій можна розділити на два класи: до першого належать методи, які використовують випадковий вибір систем булевих SAC-функцій, а до другого - детерміновані, засновані на тій чи іншій властивості SAC-функцій. На практиці частіше використовують випадковий вибір SAC-функцій, синтезованих окремо детермінованими методами. Але їх обчислювальна складність носить експоненційний характер, що обмежує використання таких методів побудовою ортогональних систем SAC-функцій від відносно невеликої кількості змінних. Основною перевагою таких методів є можливість побудови будь-якої з об'єктивно існуючих ортогональних систем SAC-функцій. Крім того, специфіка застосувань синтезується системи часто вимагає наявності додаткових властивостей, які досить просто можуть бути забезпечені в процесі підбору.

Тому важливим завданням є розробка підходів до синтезу ортогональних систем SAC-функцій, що забезпечують меншу обчислювальну складність і більшу кількість систем, які потенційно можуть бути побудовані.

3. Теоретичні основи побудови ортогональних систем SAC–функцій.

Введемо наступні позначення:

X – множина всіх n змінних: $X=\{x_1, x_2,\ldots,x_n\}$.

$\lambda(X_0)$ – булева лінійна функція від змінних множини $X_0 \subseteq X$:

$$\lambda(X_0) = a_0 \oplus \bigoplus_{\forall x_j \in X_0} a_j \cdot x_j, a_j,$$

$$a_0 \in \{0,1\}, j \in \{1,\ldots,n\} \qquad (1)$$

$H(X_0)$ – булева лінійна функція, що являє собою суму по модулю 2 всіх змінних, що належать множині X_0 :

$$H(X) = \bigoplus_{\forall x_j \in X_0} x_j = \lambda(X_0) : \forall a_j = 1, a_0 = 0 \qquad (2)$$

Вагою Гемінга булевої функції $f(X)$ називається кількість наборів змінних, на яких функція приймає одиничне значення:

$$W(f(X)) = \sum_{X_k \in Z} f(X_k)$$

Розглянемо наступний клас булевих функцій, що є окремим випадком суперпозиційних функцій при $k = 2$:

$$z(X) = H(X_1) \cdot H(X_2) \oplus \lambda(X) \quad (3)$$

де $\lambda(X) \notin \{0,1\}$, а функції $H(X_1)$ і $H(X_2)$ – це XOR непустих підмножин X_1 і X_2, що не пересікаються, об'єднання яких утворює множину всіх змінних.

Функція $z(X)$ є балансною і відповідає SAC. Функції $H(X_1)$, $H(X_2)$ і $\lambda(X)$ – лінійні і утворюють ортогональну систему. Очевидно, що $W(z(X)) = W(H(X_1) \cdot H(X_2)) + W(\lambda(X)) - 2 \cdot W(H(X_1) \cdot H(X_2) \cdot \lambda(X))$. Оскільки вага Гемінга добутку k ортогональних функцій рівна 2^{n-k-1}, то $W(z(X)) = 2^{n-3} + 2^{n-1} - 2 \cdot 2^{n-4} = 2^{n-1}$. Тобто функція $z(X)$ – балансна. Нехай змінна $x_q \in X_1$, тоді функція зміни $z(x)$ при інвертуванні змінної x_q буде мати вигляд:

$$\frac{\partial z}{\partial x_q} = z(x_1,...,x_q,...,x_n) \oplus z(x_1,...,\overline{x_q},...,x_n) = H(X_2) \oplus \delta_q$$

, причому $\delta_q=1$, якщо змінна входить в $\lambda(X)$ і $\delta_q=0$ у зворотному випадку. Ця функція балансна, оскільки збігається з лінійною функцією або її інверсією. Аналогічно можна показати, що ця властивість зберігається при $x_q \in X_2$. Таким чином, при інвертуванні будь-якої з n змінних, значення функції $z(X)$ змінюється з ймовірністю 0.5, тобто функція $z(X)$ задовольняє SAC.

Отже, необхідною і достатньою умовою для того, щоб функція (3) була балансною, є ортогональність її лінійної складової $\lambda(X)$ лінійним функціям $H(X_1)$ і $H(X_2)$.

Нехай $L(X)=\{l_1(X),l_2(X),\ldots,l_m(X)\}$, $m \le n$ – система ортогональних лінійних булевих функцій.

Розглянемо систему булевих функцій виділеного класу (3):

$$\begin{aligned} z_1(X) &= \lambda_1(X) \bullet (1 \oplus H(X)) \oplus l_1(X) \\ z_2(X) &= \lambda_2(X) \bullet (1 \oplus H(X)) \oplus l_2(X) \\ &\ldots \\ z_m(X) &= \lambda_m(X) \bullet (1 \oplus H(X)) \oplus l_m(X) \end{aligned} \quad (4)$$

Система (4) являє собою ортогональну систему SAC-функцій. Дійсно, кожна з її функцій може бути представлена у вигляді (3):

$$z_j(X) = H(X_1) \cdot H(X - X_1) \oplus l_1(X),$$
$$H(X_1) = \lambda_1(X), j \in \{1,\ldots,m\}$$

і, відповідно, вона задовольняє SAC. Система (4) ортогональна за умови ортогональності функцій лінійного базису $\{L\} = \{l_1(X), l_2(X),\ldots, l_m(X)\}$. Дійсно, XOR будь-якої підмножини G функцій системи (3) може бути представлено у вигляді XOR подвійних термів і не рівній константі лінійної функції:

$$\bigoplus_{t \in G} z_t(X) = \bigoplus_{t \in G} H(X_t) \cdot H(X - X_t) \oplus \bigoplus_{t \in G} l_t(X)$$

Відповідно, будь-яка лінійна комбінація функцій системи (4) є балансною. При цьому максимальний ступінь термів, що входять в z_i(X), $i = 1..m$ дорівнює двом. Нелінійність функцій системи (4) дорівнює 2^{n-2}.

Для більшості криптографічних застосувань важливим є те, щоб порядок нелінійності булевих функцій, що входять в ортогональну систему, був якомога більшим. Для розв'язання цієї задачі пропонується ввести додаткові перетворення над функціями системи (4) і формувати ортогональну систему SAC-функцій в наступному вигляді:

$$\begin{aligned} f_1 &= [Z]^{m-2}_{z_1,z_m} \cdot (z_1 \oplus z_m) \oplus z_1 \\ f_2 &= [Z]^{m-2}_{x_2,x_1} \cdot (z_2 \oplus z_1) \oplus z_2 \\ &\ldots \\ f_j &= [Z]^{m-2}_{z_j,z_{(j-1) \bmod m}} \cdot (z_j \oplus z_{(j-1) \bmod m}) \oplus z_j \\ &\ldots \\ f_m &= [Z]^{m-2}_{z_m,z_{m-1}} \cdot (z_m \oplus z_{m-1}) \oplus z_m \end{aligned} \quad (5),$$

де $[Z]^{m-2}_{x_i,z_j}$ – кон'юнкція m-2 функцій системи (4), крім z_i і z_j.

Для отримання ортогональних систем SAC-функцій, що володіють нелінійністю більшою в порівнянні з функціями системи (4), пропонується наступний підхід.

Нехай існує система ортогональних лінійних функцій $\{U\}^{2m-1}=\{u_1,u_2,\ldots,u_{2m-1}\}$ визначених на множині X змінних ($m<n/2$), причому функції $u_1,u_2,\ldots,u_{2m}$ включають в якості лінійних компонент всі змінні множини X. Тоді наступна функція ϕ буде балансною і задовольняти SAC, а також мати нелінійність, що дорівнює $NL(\phi)=2^{n-1}(1 - 2^{-m})$:

$$\phi(X) = u_1 \cdot u_2 \oplus u_3 \cdot u_4 \oplus \cdots \oplus u_{2 \cdot m-1} \cdot u_{2 \cdot m} \oplus u_{2 \cdot m+1} \quad (6)$$

Оскільки лінійні функції $u_1,u_2,\ldots,u_{2m-1}$ ортогональні, то функція (6) приймає одиничне значення рівно на половині всіх 2^{2m-1} наборів значень функцій u_1, u_2, ..., u_{2m-1}.

Оскільки кожен набір значень цих функцій відповідає 2^{n-2m-1} наборам значень змінних, то функція $\phi(X)$ приймає одиничне значення рівно на 2^{n-1} наборів значень змінних, тобто є балансною.

Кожна змінна $x_j \in X$, $j=1,\ldots,n$ входить в один з кон'юнктивних добутків $\phi(X)$, тому в розкладі Шеннона функції $\phi(X)$ по змінній x_j:

$$\phi(X) = x_j \cdot \psi(X - x_j) \oplus \gamma(X - x_j)$$

функція $\psi(X-x_j)$ завжди лінійна. Відповідно, функція $\phi(X)$ задовольняє SAC.

Нелінійність функції $\phi(X)$ визначається формулою:

$$N(\phi(X)) = 2^{n-1} \cdot (1 - 2^{-m})$$

Сутність запропонованого підходу для отримання ортогональних систем SAC-функцій з високою нелінійністю полягає в наступному:

Нехай для деяких цілих додатних m, $q \le m$ і парного $k < m$, існують:

- система ортогональних SAC–функцій $\{Z\}^m = \{z_1,\ldots,z_m\}$ виду (4);
- система лінійних ортогональних функцій $\{\lambda\}^q = \{\lambda_1(Z),\ldots, \lambda_q(Z)\}$;
- матриця Q розмірності $q \times k$, кожен з елементів якої є лінійною функцією, що задовольняє наступним вимогам:

a) $\forall\ i = 2\ldots q$, j = 1…k/2: $Q_{i,j*2}(Z) = Q_{1,j*2}(Z)$;

b) $\forall\ i = 1\ldots q$ система $\{S_i\}^{k\oplus 1} = \{\lambda_i(Z), Q_{i,1}(Z), Q_{i,2}(Z),\ldots,Q_{i,k}(Z)\}$ є ортогональною;

c) Неконстантні елементи множини $P^{k\square 1} = \{ a_1\lambda_1(Z) \oplus\ldots\oplus a_q\lambda_q(Z),\ a_1Q_{1,1}(Z) \oplus\ldots\oplus a_q Q_{q,1}(Z),\ldots,\ a_1Q_{1,k}(Z) \oplus\ldots\oplus a_q Q_{q,k}(Z)\}$ складають ортогональну систему S^p ($p \le k\oplus 1$ – кількість неконстантних елементів) $\forall\ a_i \in \{0,1\}$, $i=1,\ldots,q$.

Тоді наступна система буде ортогональною, її функції задовольнятимуть критерію строго лавинового ефекту і мати нелінійність рівну $N(f_i(Z)) = 2^{m-1}(1 - 2^{-k/2})$:

$$f_1(Z) = \lambda_1(Z) \oplus Q_{1,1}(Z) \cdot Q_{1,2}(Z) \oplus Q_{1,3}(Z) \cdot Q_{1,4}(Z) \oplus \cdots \oplus Q_{1,k-1}(Z) \cdot Q_{1,k}(Z)$$
$$f_2(Z) = \lambda_2(Z) \oplus Q_{2,1}(Z) \cdot Q_{2,2}(Z) \oplus Q_{2,3}(Z) \cdot Q_{2,4}(Z) \oplus \cdots \oplus Q_{2,k-1}(Z) \cdot Q_{2,k}(Z)$$
.....
$$f_q(Z) = \lambda_q(Z) \oplus Q_{q,1}(Z) \cdot Q_{q,2}(Z) \oplus Q_{q,3}(Z) \cdot Q_{q,4}(Z) \oplus \cdots \oplus Q_{q,k-1} \cdot Q_{q,k}(Z)$$

Згідно з умовою *b*) функції системи задовольняють умовам твердження 1, тому кожна з них відповідає критерію строго лавинового ефекту і має нелінійність рівну:

$$\forall j \in \{1,\ldots,q\} : N(f_j(Z)) = 2^{m-1} \cdot (1 - 2^{-k/2})$$

Розглянемо лінійну комбінацію функцій системи. Згідно з умовою *c*) можливі два варіанти:

- при $p = 1$ - лінійна комбінація функцій системи є лінійною функцією, отже, її Гемінгова вага в просторі функцій $\{Z\}^m$: $W(Z) = 2^{m-1}$;
- при $p > 1$ також $W(Z) = 2^{m-1}$.

Таким чином, будь-яка лінійна комбінація функцій системи балансна в просторі ортогональних функцій $\{Z\}^m$, це означає, що система ортогональна і в просторі змінних $\{X\}^n$.

4. Метод побудови ортогональних систем булевих функцій, що задовольняють критерію строго лавинового ефекту

Пропонується наступний метод побудови ортогональних систем з m ($m \le n$) булевих функцій від n змінних:

1. Формується перша ортогональна система з m лінійних функцій $\{G\}^m$:

$$\{G(X)\}^m = \{g_1(X), g_2(X),\ldots,g_m(X)\}$$

причому сума за модулем 2 будь-якої підмножини функцій $\{G\}^m$ не дорівнює $H(X)$ або $1\oplus H(X)$

2. Формується друга ортогональна система з m лінійних функцій $\{V\}^m$:

$$\{V(X)\}^m = \{v_1(X), v_2(X),\ldots,v_m(X)\}$$

причому мають виконуватись наступні умови:

$$\bigoplus_{j=1}^{m} b_1 \cdot v_j(X) \oplus b_0 \ne \alpha \cdot H(X) : \forall b_i \in \{0,1\}, i = 0,\ldots,m, a \in \{0,1\}$$

$$\bigoplus_{j=1}^{m} b_j \cdot (v_j(X) \oplus g_j(X)) \oplus b_0 \ne \alpha \cdot H(X) : \forall b_i \in \{0,1\}, i = 0,\ldots,m, a \in \{0,1\}$$

3. Складається наступна система $\{Z\}^m$ з m нелінійних функцій:

$$\{Z(X)\}^m : z_j(X) = g_j(X) \cdot (1 \oplus H(X)) \oplus v_j(X), j = 1,\ldots,m \quad (7)$$

Отримана в результаті система $\{Z\}^m$ є ортогональною і складається з m функцій виду (3), що задовольняють SAC-критерію, які мають нелінійність рівну $NL(z_i) = 2^{n-2}$.

При m = n з використанням запропонованого методу формується оборотне перетворення. Для формування оборотних перетворень розроблено наступний алгоритм.

Позначимо через $\underline{A}$ вектор коефіцієнтів представлення лінійної функції $\lambda(X)$ у вигляді (1): $\underline{A} = [a_n, a_{n-1},\ldots,a_2,a_1]$

Введемо позначення для операцій над двійковими векторами

shl($\underline{B}$, *j*) – логічний зсув вліво вектора $\underline{B}$ на *j* позицій;
rol($\underline{B}$, *i*) – циклічний зсув вліво вектора $\underline{B}$ на *j* позицій;
k, *q* – цілочисельні змінні

АЛГОРИТМ 1.

ПОЧАТОК.

КРОК 1. Нехай $\underline{A} = 11b$, $k = log_2(n)$, $q=1$;

КРОК 2. Обрати 2^q-бітний вектор $\underline{B}$: $W(\underline{B}) = 2^{(q-1)}$, $W(\underline{A} \oplus \underline{B}) = 2^{(q-1)}$;

КРОК 3. $\underline{A} = (\underline{A} \oplus \underline{B}) \oplus shl(\underline{B}, 2^q)$;

КРОК 4. $q = q \oplus 1$, якщо $q < k$ перейти на КРОК 2;

КРОК 5. $\{G\}^n$: $g_i(X) \equiv rol(\underline{A}, i)$, $i=1...n$;

КРОК 6. $\{V\}^n$: $v_i(X) = x_i$, $i=1...n$;

КРОК 7. $\{Z\}^n$: $z_i = g_i(X)(H(X) \oplus 1) \oplus v_i(X)$, $i=1...n$.

КІНЕЦЬ.

Булеві функціональні перетворення, побудовані наведеним алгоритмом, складаються з функцій виду (3), які мають нелінійність рівну $N(z_i) = 2^{n-2}$.

Для отримання ортогональних систем булевих функцій з більшою нелінійністю може бути використано лінійне комбінування ортогональних систем $\{Z_1(X)\}^m$, $\{Z_2(X)\}^m$,…,$\{Z_k(X)\}^m$ SAC-функцій (7):

Розглянемо наступну систему $R = \{r_1(X), r_2(X), ..., r_m(X)\}, m \le n$:

$$r_1(X) = L_1(X) \oplus Q_{1,1}(X) \cdot t_1(X) \oplus Q_{1,2}(X) \cdot t_2(X) \oplus ... \oplus Q_{1,k}(X) \cdot t_k(X)$$
$$r_2(X) = L_2(X) \oplus Q_{2,1}(X) \cdot t_1(X) \oplus Q_{2,2}(X) \cdot t_2(X) \oplus ... \oplus Q_{2,k}(X) \cdot t_k(X)$$
$$...$$
$$r_m(X) = L_m(X) \oplus Q_{m,1}(X) \cdot t_1(X) \oplus Q_{m,2}(X) \cdot t_2(X) \oplus ... \oplus Q_{m,k}(X) \cdot t_k(X) \quad (8)$$

Ортогональність цієї системи забезпечується виконанням умов, що накладаються твердженням 1. Система (8) являє собою лінійну комбінацію k систем вигляду (7):

$R = \Omega_1 \oplus \Omega_2 \oplus ... \oplus \Omega_k$

$R = \Omega_1 \oplus \Omega_2 \oplus ... \oplus \Omega_m;$

Ω_i, $i=1..m$:

$$f_1^i = Q_{1,i}(X) \cdot t_i(X) \oplus l_1^i(X)$$
$$f_2^i = Q_{2,i}(X) \cdot t_i(X) \oplus l_2^i(X)$$
$$\cdots$$
$$f_m^i = Q_{m,i}(X) \cdot t_i(X) \oplus l_m^i(X)$$

де $$L_j(X) = \bigoplus_{q=1}^{k} l_j^q(X), j = 1...m$$

Таким чином, правомірне твердження, що система *R* складається з *k* каскадів Ω_i, кожен з яких представляє собою систему вигляду (7). Міркування щодо залежності нелінійності синтезованих функцій від числа функцій вигляду (3) в їх складі можуть бути без порушення загальності поширені на системи (8), де нелінійність залежить від числа каскадів.

Для побудови систем вигляду (8) пропонується наступний каскадний метод.

1. Задати *k* різних множин змінних X_i, $i = 1 ... k$, об'єднання яких дає множину всіх змінних $X = X_1 \cup X_2 \cup \ldots \cup X_k$. Причому, лінійні функції, що являють собою суми всіх змінних підмножин *Xi*, складають ортогональну систему булевих функцій: $\{H(X_1), H(X_2), ..., H(X_m)\}$.
2. Скласти ортогональну лінійну систему *m* функцій Λ, визначених на множині змінних *X*:

$\Lambda = \{L_1(X), L_2(X), ..., L_s(X)\}$, причому:

$$\bigoplus_{i=1}^{m} L_i(X) \cdot b_i \ne b_0 \oplus \alpha \cdot H(X), \forall \alpha, b_j \in \{0,1\}, j = 0,...,m$$

3. Скласти *k* лінійних систем P^j, $j = 1 ... k$ з *m* функцій, визначених на множинах X_j відповідно:

$$P^j = \{p_1^j(X_j), p_2^j(X_j), ..., p_m^j(X_j)\}, j = 1,...,k,$$

причому:

$$\bigoplus_{j=1}^{k} (b_1 \cdot p_1^j(X_j) \oplus b_2 \cdot p_2^j(X_j) \oplus \cdots \oplus b_k \cdot p_m^j(X_j)) \cdot (1 \oplus H(X_j)) \oplus$$
$$\oplus b_1 \cdot L_1(X) \oplus b_2 \cdot L_2(X) \oplus \cdots \oplus b_m \cdot L_m(X) \ne \alpha, \forall a, b_i \in \{0,1\}, i = 1,...,m$$

4. Скласти результуючу систему:

$$r_1(X) = L_1(X) \oplus p_1^1(X) \cdot (1 \oplus H(X_1)) \oplus p_1^2(X) \cdot (1 \oplus H(X_2)) \oplus \cdots \oplus p_1^k(X) \cdot (1 \oplus H(X_k))$$
$$r_2(X) = L_2(X) \oplus p_2^1(X) \cdot (1 \oplus H(X_1)) \oplus p_2^2(X) \cdot (1 \oplus H(X_2)) \oplus \cdots \oplus p_2^k(X) \cdot (1 \oplus H(X_k))$$
$$...$$
$$r_m(X) = L_m(X) \oplus p_m^1(X) \cdot (1 \oplus H(X_1)) \oplus p_m^2(X) \cdot (1 \oplus H(X_2)) \oplus \cdots \oplus p_m^k(X) \cdot (1 \oplus H(X_k))$$

Результуюча система є ортогональною, а складові її функції задовольняють SAC і мають нелінійність рівну:

$N_r = 2^{n-1} \cdot (1 - 2^{-k}`)$.

Як приклад використання викладеного методу розглянемо побудову восьми ортогональних булевих SAC-функцій від 8-ми змінних (оборотного *S*-блоку на 8 входів).

Етап I

Задамо множини змінних $X_1, \ldots, X_m$.

Для отримання максимально нелінійного перетворення використовуємо три каскада (*k* =

3). Одна з множин має бути повною, щоб забезпечити можливість побудови невиродженої системи восьми функцій.

$X_1 = \{x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8\}$;
$X_2 = \{x_1,x_2,x_3,x_4\}$;
$X_3 = \{x_1,x_6,x_7,x_8\}$.

Етап II
Складемо невироджені системи на множинах змінних X_1, X_2, X_3. Скористаємося запропонованим вище алгоритмом (кроки 1-6) для отримання першого каскада синтезованої системи. Другий і третій каскади можуть бути отримані аналогічно.
Линейная функция, представляющая собой XOR всех переменных множества X_1:

$$H(X_1) = x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus x_7 \oplus x_8.$$

Система булевих функцій, визначених на множині змінних X_1 (перший каскад):

ПОЧАТОК.
КРОК 1. $\underline{A} = 11b$, $c = 3$, $d=1$;
КРОК 2.1 $\underline{B} = 10b$;
КРОК 3.1 $\underline{A} = (\underline{A} \oplus \underline{B}) \oplus shl(\underline{B}, 2^d) = 1001b$;
КРОК 4.1 $d = d \oplus 1 = 2$;
КРОК 2.2 $\underline{B} = 1100b$;
КРОК 3.2 $\underline{A} = (\underline{A} \oplus \underline{B}) \oplus shl(\underline{B}, 2^d) = 11000101b$;
КРОК 4.2 $d = d \oplus 1 = 3$;
КРОК 5. P:
$p_1^1(X) = 11000101b$;
$p_2^1(X) = 10001011b$;
$p_3^1(X) = 00010111b$;
$p_4^1(X) = 00101110b$;
$p_5^1(X) = 01011100b$;
$p_6^1(X) = 10111000b$;
$p_7^1(X) = 01110001b$;
$p_8^1(X) = 11100010b$;
КІНЕЦЬ.

Таким чином, перший каскад Ω_1 (система восьми функцій виду (3) на множині змінних X_1) матиме вигляд:

$$f_1(X) = (x_1 \oplus x_3 \oplus x_7 \oplus x_8)(x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus x_7 \oplus x_8 \oplus 1);$$
$$f_2(X) = (x_1 \oplus x_2 \oplus x_4 \oplus x_8)(x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus x_7 \oplus x_8 \oplus 1);$$
$$f_3(X) = (x_1 \oplus x_2 \oplus x_3 \oplus x_5)(x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus x_7 \oplus x_8 \oplus 1);$$
$$f_4(X) = (x_2 \oplus x_3 \oplus x_4 \oplus x_6)(x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus x_7 \oplus x_8 \oplus 1);$$
$$f_5(X) = (x_3 \oplus x_4 \oplus x_5 \oplus x_7)(x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus x_7 \oplus x_8 \oplus 1);$$
$$f_6(X) = (x_4 \oplus x_5 \oplus x_6 \oplus x_8)(x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus x_7 \oplus x_8 \oplus 1);$$
$$f_7(X) = (x_1 \oplus x_5 \oplus x_6 \oplus x_7)(x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus x_7 \oplus x_8 \oplus 1);$$
$$f_8(X) = (x_2 \oplus x_6 \oplus x_7 \oplus x_8)(x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus x_7 \oplus x_8 \oplus 1).$$

Повні лінійні функції на X_2 і X_3 відповідно:

$$H(X_2) = x_1 \oplus x_2 \oplus x_3 \oplus x_4;$$
$$H(X_3) = x_1 \oplus x_6 \oplus x_7 \oplus x_8.$$

Візьмемо ортогональні попереднім функції:

$$p_i^2(X) = x_1 \oplus x_3$$
$$p_i^3(X) = x_6 \oplus x_8, \quad i=1..8$$

В якості лінійної системи визначеної на повній множині вхідних змінних візьмемо $L_i(X) = x_i$, i=1..8.

Етап III
Складемо систему вигляду (8) з трьох каскадів:

$$f_1(X) = (x_1 \oplus x_3 \oplus x_7 \oplus x_8)(x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus x_7 \oplus x_8 \oplus 1) \oplus (x_1 \oplus x_3)(x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus 1) \oplus (x_6 \oplus x_8)(x_1 \oplus x_6 \oplus x_7 \oplus x_8 \oplus 1) \oplus x_1;$$
$$f_2(X) = (x_1 \oplus x_2 \oplus x_4 \oplus x_8)(x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus x_7 \oplus x_8 \oplus 1) \oplus (x_1 \oplus x_3)(x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus 1) \oplus (x_6 \oplus x_8)(x_1 \oplus x_6 \oplus x_7 \oplus x_8 \oplus 1) \oplus x_2;$$
$$f_3(X) = (x_1 \oplus x_2 \oplus x_3 \oplus x_5)(x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus x_7 \oplus x_8 \oplus 1) \oplus (x_1 \oplus x_3)(x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus 1) \oplus (x_6 \oplus x_8)(x_1 \oplus x_6 \oplus x_7 \oplus x_8 \oplus 1) \oplus x_3;$$
$$f_4(X) = (x_2 \oplus x_3 \oplus x_4 \oplus x_6)(x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus x_7 \oplus x_8 \oplus 1) \oplus (x_1 \oplus x_3)(x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus 1) \oplus (x_6 \oplus x_8)(x_1 \oplus x_6 \oplus x_7 \oplus x_8 \oplus 1) \oplus x_4;$$
$$f_5(X) = (x_3 \oplus x_4 \oplus x_5 \oplus x_7)(x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus x_7 \oplus x_8 \oplus 1) \oplus (x_1 \oplus x_3)(x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus 1) \oplus (x_6 \oplus x_8)(x_1 \oplus x_6 \oplus x_7 \oplus x_8 \oplus 1) \oplus x_5;$$
$$f_6(X) = (x_4 \oplus x_5 \oplus x_6 \oplus x_8)(x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus x_7 \oplus x_8 \oplus 1) \oplus (x_1 \oplus x_3)(x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus 1) \oplus (x_6 \oplus x_8)(x_1 \oplus x_6 \oplus x_7 \oplus x_8 \oplus 1) \oplus x_6;$$

$f_7(X) = (x_1 \oplus x_5 \oplus x_6 \oplus x_7)(x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus x_7 \oplus x_8 \oplus 1) \oplus (x_1 \oplus x_3)(x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus 1) \oplus (x_6 \oplus x_8)(x_1 \oplus x_6 \oplus x_7 \oplus x_8 \oplus 1) \oplus x_7;$
$f_8(X) = (x_2 \oplus x_6 \oplus x_7 \oplus x_8)(x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus x_7 \oplus x_8 \oplus 1) \oplus (x_1 \oplus x_3)(x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus 1) \oplus (x_6 \oplus x_8)(x_1 \oplus x_6 \oplus x_7 \oplus x_8 \oplus 1) \oplus x_8.$

Розкривши дужки і скоротивши доданки, отримаємо наступне восьмирозрядне перетворення:

$f_1(X) = x_8x_7 \oplus x_8x_6 \oplus x_8x_5 \oplus x_8x_4 \oplus x_8x_2 \oplus x_8x_1 \oplus x_7x_5 \oplus x_7x_4 \oplus x_7x_2 \oplus x_6x_3 \oplus x_5x_3 \oplus x_5x_1 \oplus x_1$
$f_2(X) = x_8x_6 \oplus x_8x_5 \oplus x_8x_3 \oplus x_8x_1 \oplus x_7x_6 \oplus x_7x_4 \oplus x_7x_2 \oplus x_7x_1 \oplus x_6x_4 \oplus x_6x_2 \oplus x_5x_4 \oplus x_5x_2 \oplus x_5x_1 \oplus x_4x_1 \oplus x_3x_1 \oplus x_2x_1 \oplus x_2$
$f_3(X) = x_8x_7 \oplus x_8x_5 \oplus x_8x_3 \oplus x_8x_2 \oplus x_7x_6 \oplus x_7x_5 \oplus x_7x_3 \oplus x_7x_2 \oplus x_7x_1 \oplus x_6x_5 \oplus x_6x_3 \oplus x_6x_2 \oplus x_5x_4 \oplus x_4x_2 \oplus x_3x_2 \oplus x_3 \oplus x_2x_1$
$f_4(X) = x_8x_7 \oplus x_8x_6 \oplus x_8x_4 \oplus x_8x_3 \oplus x_8x_2 \oplus x_8x_1 \oplus x_7x_4 \oplus x_7x_3 \oplus x_7x_2 \oplus x_6x_5 \oplus x_5x_4 \oplus x_5x_3 \oplus x_5x_2 \oplus x_4x_3 \oplus x_4 \oplus x_3x_2 \oplus x_3x_1$
$f_5(X) = x_8x_5 \oplus x_8x_4 \oplus x_8x_3 \oplus x_8x_1 \oplus x_7x_2 \oplus x_7x_1 \oplus x_6x_5 \oplus x_6x_4 \oplus x_6x_3 \oplus x_6x_1 \oplus x_5x_2 \oplus x_5x_1 \oplus x_5 \oplus x_4x_3 \oplus x_4x_2 \oplus x_3x_1 \oplus x_2x_1$
$f_6(X) = x_8x_3 \oplus x_8x_2 \oplus x_7x_5 \oplus x_7x_4 \oplus x_6x_3 \oplus x_6x_2 \oplus x_6 \oplus x_5x_3 \oplus x_5x_2 \oplus x_5x_1 \oplus x_4x_2 \oplus x_3x_2 \oplus x_2x_1$
$f_7(X) = x_8x_6 \oplus x_8x_5 \oplus x_7x_6 \oplus x_7x_4 \oplus x_7x_3 \oplus x_7x_2 \oplus x_7 \oplus x_6x_4 \oplus x_6x_3 \oplus x_6x_2 \oplus x_6x_1 \oplus x_5x_4 \oplus x_5x_3 \oplus x_5x_2 \oplus x_4x_3 \oplus x_3x_2 \oplus x_3x_1$
$f_8(X) = x_8x_7 \oplus x_8x_5 \oplus x_8x_4 \oplus x_8x_3 \oplus x_8 \oplus x_7x_6 \oplus x_7x_5 \oplus x_7x_4 \oplus x_7x_3 \oplus x_7x_1 \oplus x_6x_5 \oplus x_6x_4 \oplus x_6x_3 \oplus x_5x_2 \oplus x_4x_3 \oplus x_4x_2 \oplus x_4x_1$

Перетворення є оборотним, оскільки система ортогональна і m = n. Функції, що складають перетворення, відповідають критеріям строго лавинового ефекту і мають нелінійність рівну 112 (максимальна для восьми змінних 120).

5. Висновок

На основі проведених теоретичних досліджень ортогональних систем булевих функцій сформульовано і доведено ряд їх властивостей, які можуть бути використані для створення ефективного методу синтезу систем функцій, що володіють лавиновим ефектом.

Характерна особливість розробленого каскадного методу полягає в можливості балансування нелінійності синтезованих систем ортогональних булевих функцій і, відповідно, обчислювальної складності їх реалізації.

УДК 004.2

СКОРІЧЕНКО О.В.
ЖАБІН В.І.,

СКОРОЧЕННЯ НЕОБХІДНОГО РЕСУРСУ ПЛІС ДЛЯ РЕАЛІЗАЦІЇ ОБЧИСЛЮВАЛЬНИХ СИСТЕМ З БЕЗПОСЕРЕДНІМИ ЗВ'ЯЗКАМИ МІЖ МОДУЛЯМИ

Запропоновано метод обчислення поліномів з порозрядною обробкою операндів у надлишковому поданні в системах з безпосередніми зв'язками між обчислювальними модулями. Використання зазначеного методу дозволяє скоротити необхідний ресурс ПЛІС завдяки малому числу зв'язків між компонентами системи.

A method is proposed for computing polynomials with bitwise processing of operands in redundant representation in systems with direct connections between computational modules. The use of this method allows to reduce the required resource of the FPGA due to the small number of connections between system components.

1. Вступ

Тривалість обробки інформації у паралельних системах залежить не тільки від часу виконання операцій, але і від затрат часу на обмін інформацією між гілками алгоритмів, тобто між обчислювальними модулями (ОМ) паралельної системи. Зменшити затрати часу на обмін даними дозволяє використання потокових систем з безпосередніми зв'язками (ПСБЗ) між ОМ [1, 2].

У ПСБЗ виходи одних ОМ підключаються до входів інших ОМ відповідно до графа потоку даних (ГПД). ОМ працюють у неавтономному режимі. У процесі обчислень дані пересилаються безпосередньо від одних ОМ до інших, перетворюючись на кожному кроці відповідно до операцій, що задані вершинами ГПД. У такому випадку відсутні складні процедури пересилання даних між ОМ через загальну пам'ять, тобто зменшуються затрати часу на обмін даними між ними. Формалізовані методики переходу від ГПД до структури ПСБЗ відомі [3-5].

Використання сучасної технології проектування RSoC (Reconfigurable system on a chip – реконфігурована система на кристалі) дозволяє створювати складні системи на основі ПЛІС. Однак, з боку ресурсів мікросхем накладається ряд обмежень. При паралельній передачі інформації між мікросхемами виникають проблеми, пов'язані з можливою нестачею виводів, а в середині мікросхеми суттєво витрачається внутрішній ресурс функціональних елементів та елементів зв'язку. Зростає енергоспоживання і збільшуються габаритні розміри системи. Тому більш ефективним є порозрядний обмін даними.

Використання декількох мікросхем створює додаткові проблеми. Недоліком такої реалізації є те, що мікросхеми можуть не мати необхідної кількості виводів для забезпечення зв'язків між частинами системи. При цьому частина ресурсів мікросхем може залишатися незадіяною.

З огляду на важливість проблеми нестачі виводів мікросхем, компанією Virtual Machine Works запропонована технологія VirtualWire (віртуальні з'єднання) для побудови систем на декількох мікросхемах [6]. Ідея, закладена в основі технології, полягає у

використанні незадіяного обладнання для реалізації спеціальних ланцюгів, що забезпечують почергове підключення до виводів мікросхеми інформації з різних джерел всередині мікросхеми. До недоліків даної технології слід віднести великі часові затримки просування потоків даних, що суперечить самій ідеї потокової моделі обчислень.

2. Постановка задачі

Одним з підходів до вирішення проблеми зменшення кількості зв'язків між ОМ є використання квазіпаралельних обчислювальних пристроїв, що дозволяють суміщати процеси порозрядного введення операндів і порозрядного формування результатів [5, 7]. Подання чисел в надлишкових системах числення неоднозначне, тобто одне і те ж число може бути записане різними послідовностями цифр. Наприклад, десяткове число 5/16 в двійковій системі з цифрами {-1,0,1} можна подати у вигляді: 0,0101; $0,1\bar{1}01$; $0,011\bar{1}$ і т.д. (тут «$\bar{1}$» – інший запис цифри «-1»). Це дозволяє виконувати операції порозрядно без переносів у старші розряди. Режим роботи таких ОМ називають неавтономним, бо для виконання послідовності операцій необхідно кілька ОМ, які обмінюються інформацією у процесі роботи.

Хоча на входах і виходах ОМ числа представлені послідовним кодом, такі пристрої по внутрішній організації ближчі до паралельних пристроїв. У зв'язку з цим вони отримали назву квазіпаралельні [2, 7]. З використанням квазіпаралельних ОМ при виконанні послідовності залежних за даними операцій реалізується паралелізм на рівні обробки розрядів операндів.

У даній роботі на прикладі ПСБЗ для обчислення поліномів досліджується можливість скорочення апаратних ресурсів ПЛІС за рахунок використання квазіпаралельних ОМ відносно використання ОМ з паралельним обміном даних.

3. Організація обчислення поліномів

Процес виконання в часі послідовності операцій у неавтономному режимі ілюструється діаграмою на рис. 1.

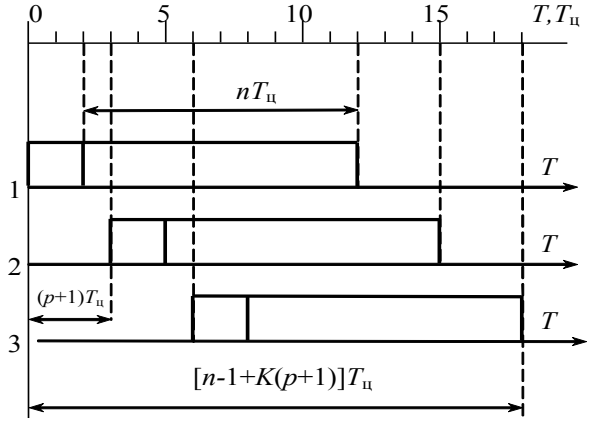

Рис. 1. Часова діаграма виконання залежних операцій в 3-х ОМ

Операції виконуються зі старших розрядів за допомогою ланцюга ОМ, що формують цифри проміжних результатів із затримкою на p циклів кожний. Наступний у ланцюгу ОМ починає свою операцію через $(p+1)$ циклів відносно попереднього ОМ. Це означає, що час обчислень, необхідний для отримання остаточного результату, складає

$$T = \left[n - 1 + \sum_{j=1}^{K} \left(p_j + 1 \right) \right] t_{\text{Ц}}, \qquad (1)$$

де n – розрядність операндів і результату; k–число операцій у ланцюгу; p_j– затримка формування розрядів результату j-ї операції; $t_Ц$ – тривалість циклу формування одного розряду результату в ОМ.

Для обчислення поліномів скористаємося методом Горнера першого порядку. Наприклад, поліном 5-го порядку можна записати у вигляді

$$P(x, a_i) = ((((a_5 x + a_4)x + a_3)x + a_2)x + a_1)x + a_0$$

Перший підхід. Поліном можна обчислити методом певної суперпозиції операцій множення і додавання. В двійковій системі числення з цифрами {-1,0,1} алгоритм виконання додавання та множення для правильних дробових чисел в *i*-му циклі може бути зведений до наступних дій [7]:

$$H_i = 2R_{i-1} + F_i, \qquad (2)$$

$$z_i = \begin{cases} -1, \text{ якщо } H_i < -2^{-1}; \\ 0, \text{ якщо } -2^{-1} \le H_i \le 2^{-1}; \\ 1, \text{ якщо } 2^{-1} < H_i, \end{cases} \qquad (3)$$

$$R_i = H_i - z_i, \qquad (4)$$

де H_i, R_i – проміжні змінні; F_i – приріст функції, що залежить від *i*-х цифр операндів; z_i – цифра результату. Початковим є значення $R_0=0$.

Приріст F_i для операції додавання та множення обчислюється за формулами:

$F_i=2^{-p}(x_i + y_i)$,

$$F_i=2^{-p}(x_iY_{i-1} + y_iX_{i-1}), \qquad (5)$$

де p – затримка початку формування розрядів результату в циклах; x_i і y_i – цифри операндів з вагою 2^{-i}; Y_i і X_i. – операнди, що подані i старшими розрядами. В [7] показано, що для даних операцій маємо $p \ge 2$.

Якщо множення і додавання виконувати в окремих ОМ, зв'язаних послідовно (всього в ланцюжку десять ОМ), то час обчислювання в синхронному режимі згідно з (1) буде складати

$$T = (n + 29)\, t_{\text{М}}, \qquad (6)$$

де $t_{\text{М}}$ – тривалість циклу множення (більшого за цикл додавання).

Другий підхід. Кількість циклів обчислення поліномів можна зменшити, якщо використовувати ОМ, що виконують більш складну операцію.

Нехай система являє собою ланцюжок з 5-ти ОМ, кожен з яких виконує проміжну операцію $Z = XY + A$ (рис. 2).

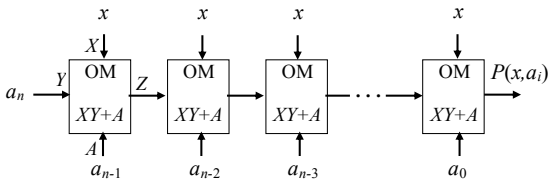

Рис. 2. Система для обчислення поліномів $P(x, a_i)$ за схемою Горнера

Будемо вважати, що операнди є нормалізованими дробовими числами і подані у формі:

$$X = \sum_{i=1}^{n} x_i 2^{-i}, \quad Y = \sum_{i=1}^{n} y_i 2^{-i}, \quad A = \sum_{i=1}^{n} a_i 2^{-i}, \qquad (7)$$

де $x_i, y_i, a_i \in \{-1,0,1\}$ – цифри операндів.

Вимагатимемо, щоб похибка результату була знакозмінною і за абсолютною величиною не перевищувала половини ваги n-го розряду після коми. Ця вимога буде виконуватися, якщо на i-му кроці цифру z_i результату вибирати таким чином, щоб мало місце співвідношення

$$Z_i - 2^{-i-1} \le 2^{-p}(X_iY_i + A_i) < Z_i + 2^{-i-1}, \qquad (8)$$

де p – число кроків затримки формування цифр результату.

Використовуючи методику, подану в [7], та формули (7), (8), можна отримати алгоритм обчислення Z у неавтономному режимі, що відповідає формулам (2)-(4). У даному випадку $p = 3$. Отже, для

отримання n розрядів результату після коми необхідно виконати $n+3$ кроків обчислення.

Більш докладніше алгоритм обчислення функції Z можна подати в наступній формі:

1. X_0, Y_0, R_0 надати значення 0.
2. Для $i = \overline{1, n+3}$ виконувати пункти 3-7.
3. $H_i = 2R_{i-1} + 2^{-3} X_{i-1} y_i + 2^{-3} Y_{i-1} x_i + 2^{-3} a_i + 2^{-3-i} x_i y_i$.
4. $X_i = X_{i-1} + x_i 2^{-i}$.
5. $Y_i = Y_{i-1} + y_i 2^{-i}$.
6. $z_i = \begin{cases} -1, \text{ якщо } H_i < -2^{-1}; \\ 0, \text{ якщо } -2^{-1} \le H_i < 2^{-1}; \\ 1, \text{ якщо } 2^{-1} \le H_i. \end{cases}$
7. $R_i = H_i - z_i$.

Тут H_i і R_i – допоміжні змінні.

В даному випадку час обчислення поліномів буде визначатися формулою

$$T = (n + 19)\, t_\Phi, \qquad (9)$$

де t_Φ – тривалість циклу формування розряду результату функції Z.

Значення t_Φ несуттєво перевищує t_M, що видно з порівняння формул для обчислення змінної H_i (див. формули (2) і (5) та п. 3 наведеного алгоритму). Це доводить ефективність використання ОМ, що реалізують функцію Z.

4. Порівняння апаратурних витрат для різних реалізацій обчислювального модуля

Для порівняльної оцінки витрат ресурсів ПЛІС при використанні пристроїв з паралельною і послідовною передачею даних при обчисленні Z проведено моделювання двох варіантів реалізації обчислювачів на базі мікросхеми EP2C35F672C6 сімейства Cyclone II фірми Altera у середовищі проектування Quartus II Version 9.1 Build 304. Результати моделювання, відповідно до звітів про компіляцію, наведені у табл. 1 (через роздільник показаний відповідно ресурс для побудови обчислювачів і загальний ресурс ПЛІС певного виду).

Табл. 1. Використовувані ресурси ПЛІС

Ресурс ПЛІС	Блок обробки операндів	
	Паралельний	Квазіпаралельний
Логічні елементи	502/33216 (1,5%)	695/33216 (2%)
Регістри	0/33216 (0%)	271/33216 (0,8%)
Блоки множення	32/70 (46%)	0/70 (0%)
Виводи	256/475 (54%)	10/475 (2%)

Для паралельного блоку помножувач 64x64 реалізований на базі вбудованих у ПЛІС швидкодіючих блоків множення.

На підставі отриманих результатів з табл. 1 можна зробити висновок, що витрати ресурсів ПЛІС більші для пристрою паралельного типу. З огляду на те, що при даній організації обчислень практично половина виводів ПЛІС використовується тільки для одного каскаду обчислювача поліномів, застосування режиму паралельного введення операндів навряд чи є доцільним. Більш реальним є режим попереднього введення у визначеному порядку 64-розрядних операндів з подальшою їх обробкою у паралельному пристрої. Час обчислення поліномів буде визначатися режимом введення операндів.

5. Висновки

Досліджена можливість підвищення ефективності систем з безпосередніми зв’язками між ОМ за рахунок реалізації неавтономних обчислень при порозрядній передачі даних між модулями системи.

У порівнянні з системами, в яких передача даних між ОМ проводиться паралельним кодом, для реалізації систем з порозрядною обробкою даних на базі квазіпаралельних ОМ потрібно менше ресурсів ПЛІС. Заощаджуються ресурси ПЛІС, збільшується ймовірність розміщення системи на одній мікросхемі, що забезпечує підвищення надійності системи, зменшення енергоспоживання та габаритів. Обмін даними між ОМ всередині мікросхеми виконується швидше, ніж між компонентами системи, що реалізовані на різних мікросхемах. Це дає потенційну можливість підвищити частоту тактування, що, у свою чергу, прискорює обробку інформації.

Таким чином, отримані результати підтверджують ефективність застосування неавтономних методів порозрядної обробки інформації в обчислювальних системах на кристалі.

Список літератури

1. Жабин В.И. Эффективность потоковых вычислений в системах с непосредственными связями, реализованных на ПЛИС / В.И.Жабин, В.В.Жабина, М.А. Безгинский // Вісник НТУУ "КПІ". Інформатика, управління та обчислювальна техніка: Зб. наук. праць. – К.: ВЕК+. – 2012. – №55. – С. 149-156.

2. Жабин В.И. Выполнение последовательностей зависимых операций в режиме совмещения / В.И.Жабин. // Вісник НТУУ «КПІ». Інформатика, управління та обчислювальна техніка: Зб. Наук. Пр. – К.: Век+. – 2007. – №46. – С. 226-233.

3. Жабин В.И. Построение быстродействующих специализированных вычислителей для реализации многоместных выражений / В.И.Жабин, В.И.Корнейчук, В.П.Тарасенко // Автоматика и вычислительная техника. – 1981. – №6. – с. 18-22.

4. Палагин А.В. Реконфигурируемые вычислительные системы: Основы и приложения / А.В. Палагин, В.Н. Опанасенко. – К.: Просвіта, 2006, 280 с.

5. Каляев И.А. Архитектура семейства реконфигурируемых вычислительных систем на основе ПЛИС / И.А. Каляев, И.И. Левин, Е.А. Семерников // Искусственный интеллект. – 2008. - № 3. – с. 663-674.

6. Максфилд К. Проектирование на ПЛИС. Архитектура, средства и методы / К.Максфилд. – М.: Издательский дом «Додэка-XXI», 2007, 408 с.

7. Жабин В.И. Некоторые машинные методы вычисления рациональных функций многих аргументов / В.И. Жабин, В.И.Корнейчук, В.П.Тарасенко // Автоматика и телемеханика. – 1977. – №12. – С. 145-154.

УДК 004.7

СТОРОЖУК В.О.,
ДОЛГОЛЕНКО О.М.

РЕКОНФІГУРОВАНИЙ ПОМНОЖУВАЧ ЧИСЕЛ З ПЛАВАЮЧОЮ КРАПКОЮ

В даній статті описана реалізація помножувача з реконфігурованою структурою для виконання операцій з плаваючою крапкою. Помножувач має однорідну структуру. Він реалізований як набір комбінаційних схем, без використання елементів пам'яті й не потребує мікропрограмного керування.

This article describes the implementation of reconfigurable multiplier structure to perform floating point. Multiplier has a homogeneous structure. It is implemented as a set of combinational circuits without using memory elements and do not require firmware control.

1. Вступ

Операція перемноження чисел в формі з плаваючою крапкою є однією з найбільш уживаних операцій, що виконується в мікропроцесорному ядрі. У зв'язку з цим від швидкості виконання цієї операції в значній мірі залежить швидкодія всього мікропроцесорного ядра.

Безліч цілих чисел нескінченна, але ми завжди можемо підібрати таке число біт, щоб представити будь-яке ціле число, що виникає при вирішенні конкретної задачі. Безліч дійсних чисел не тільки нескінченна, але ще і безперервна, тому, скільки б ми не взяли біт, ми неминуче зіткнемося з числами, які не мають точного представлення. Числа з плаваючою комою - один з можливих способів представлення дійсних чисел, який є компромісом між точністю і діапазоном прийнятих значень.

Стандарт IEEE 754 [1] представляє числа з плаваючою крапкою як десяткові числа з основою 2 в експоненційному форматі. В IEEE числу з плаваючою крапкою (Рис.1) виділяється 1 біт на знак, 8 біт на порядок і 23 біта на мантису, або дробову частину числа. Порядок розшифровується як ціле число без знака, що допускає як додатну, так і від'ємну експоненти [1]. Дріб представляється як 24 бітове двійково-десяткове (основа 2) число, де найстарший біт відповідає значенню 1 (2^0), наступний біт ½ (2^{-1}), і так далі. Двійкова крапка в уявленні мантиси завжди розташована після біта *MSB*-найбільшого значущого біту мантиси [1]. При нормалізації результату виконання арифметичної операції мантиса результату зсувається вліво або вправо, з відповідною корекцією значення порідку [6], поки в абсолютному значенні мантиси *MSB* не буде дорівнювати 1. Це значення не зберігається в пам'яті, а відновлюється в арифметичному пристрої перед виконанням операції.

Для плаваючої крапки з подвоєною точністю на порядок виділяється 11 біт, а на мантису - 52 біт. Формат числа з плаваючою крапкою IEEE показаний на Рис. 1.

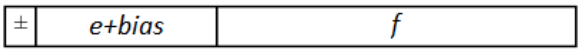

Рис. 1 Формат представлення чисел з плаваючою крапкою

2. Розробка блоку помножувача мантис з реконфігурованою структурою

Розроблюваний блок помножувача мантис орієнтований на обробку всіх форматів чисел з плаваючою крапкою, що передбачені стандартом IEEE Std 754™. Таких форматів п'ять: половинна точність (SF) - 16 розрядів, одинарна точність (F) - 32 розряда, подвійна точність (DF) - 64 розряда, подвійна розширена точність (DEF) - 80 розрядів та учетверину точність (QF) (128 розрядів). Для досягнення цієї мети блок помножувача мантис повинен мати можливість оброблювати, відповідно формату: 12, 25, 54, 66 та 114 бітні мантиси (разом із знаковим та прихованим бітом). Для побудови такого універсального швидкого помножувача мантис, без використання засобів мікропрограмного управління, найбільше підходить алгоритм *Baugh-Wooley* [2]. У алгоритмі Бо-Вулі добуток чисел в

доповняльному коді записується наступним чином:

$$A \times B = -2^{2n-1} + \left(\overline{a_{n-1}} + \overline{b_{n-1}} + \right.$$
$$\left. + a_{n-1}b_{n-1}\right) \times 2^{n-2} + \sum_{i=0}^{n-2}\sum_{j=0}^{n-2} a_i b_j \times 2^{i+j} +$$
$$+ a_{n-1}\sum_{j=0}^{n-2} 2^{n+j-1} + b_{n-1}\sum_{i=0}^{n-2} \overline{a_i} \times 2^{n+i-1} +$$
$$+ (a_{n-1} + b_{n-1}) \times 2^{n-1}$$

Часткові добутки зводяться до такого вигляду, який забезпечує максимальну регулярність масиву, що дуже зручно при мікросхемній реалізації. По ходу множення часткові добутки (ЧД), що мають знак «мінус», зсуваються до останньої ступені підсумовування. Операція віднімання ЧД заміняється додаванням їх інвертованих значень. Недоліком схеми можна вважати те, що в останньому рядку матриці необхідний додатковий суматор, через що регулярність схеми порушується. Загалом, у схемі використовується *n(n-2)+4* повних суматорів та *(n-1)* напівсуматорів.

Розглянемо роботу схеми на прикладі виконання операції помноження мантис: *p=x*y*.

Реконфігурування блоку помножувача мантис на обробку потрібного формату операндів здійснюється шляхом доповнення молодших розрядів мантис x та y нулями до розміру мантиси за форматом QF. Таким чином, в блоці помножувача мантис завжди виконується перемноження мантис *114*114*. Доповнені до формату *QF* мантиси *x* та *y* повинні подаватися на входи блока помножувача мантис так, як це показано на схемі з рис. 2.

Схема помножувача мантис складається з 114*114 двухвходових елементів &, на кожному з котрих обчислюється один розряд проміжних добутків (деякі з цих елементів, відповідно до алгоритма *Baugh-Wooley*, на рис. 3 змінені на елементи *NOT-&*). Обчислені таким чином розряди проміжних добутків підсумовуються за допомогою однорозрядних повних суматорів (*FA-full adder* на рис. 2).

Обчислений за алгоритмом Baugh-Wooley добуток потребує корекції. У нашому випадку корекція добутку полягає в тому, що в 0-ий та 113-ий розряди добутку повинна бути добавлена «1», як це показано на рис. 2.

На заключному етапі перемноження мантис здійснюється розповсюдження переносів в старшій половині обчисленого добутку. Для цього використовується суматор з обхідними переносами, схема якого приведена на рис. 3.

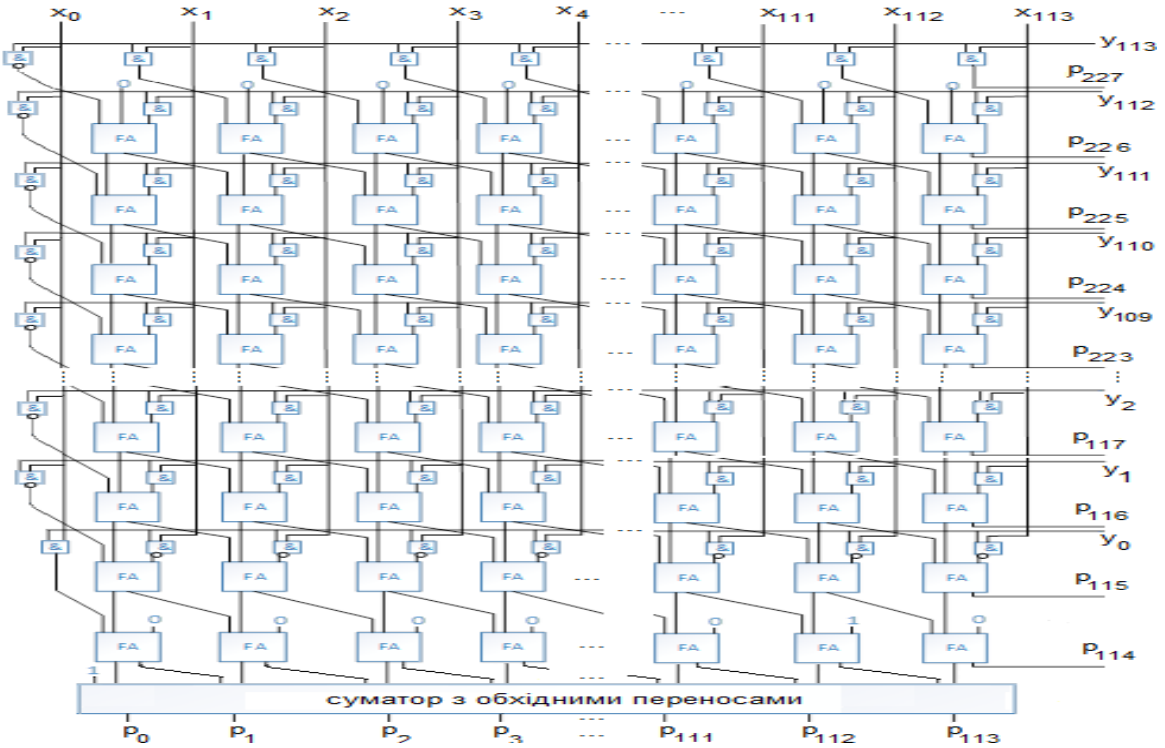

Рис. 2 Функціональна схема блоку помножувача мантис з реконфігурованою структурою

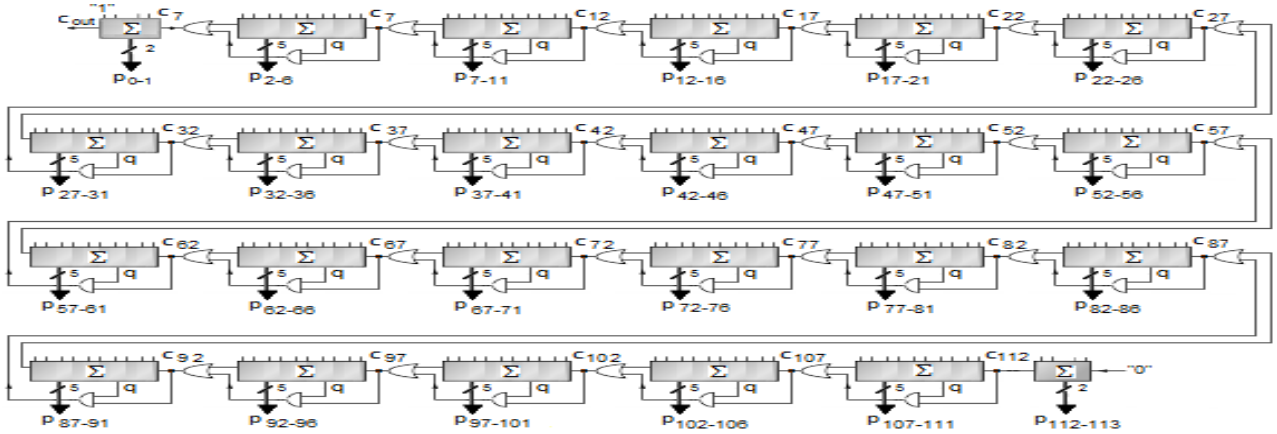

Рис.3 Функціональна схема суматора з обхідними переносами з блоку помножувача мантис

Ідея побудови такого суматора полягає в розбитті схеми *n* –розрядного суматора на групу суматорів меншого розміру, так на схемі з рис. 2 114–розрядний суматор розбитий на 22 п'ятирозрядних суматора всередині та 2 двухрозрядних суматора по краям. Кожен з таких суматорів реалізується за схемою суматора з наскрізними переносами, але відрізняється тим,

що в усіх цих суматорах, крім крайніх, додатково підраховується функція:

$$q = q_0 \& q_1 \& q_2 \& q_3 \& q_4,$$

де: $q_i = a_i \vee b_i$, a_i та b_i - двійкові сигнали на входах i – го розряду п’ятирозрядних суматорів.

Значення функції q використовується для організації обходу вхідним переносом свого суматора, одночасно з його наскрізним розповсюдженням.

Як тільки вихідний перенос з менш значущого суматора сформований, він не тільки подається на вхід перенесення наступного суматора, але також через логічний елемент *І* (якщо сформоване в цьому суматорі $q = 1$) подається і на вхід перенесення наступного суматора і т. д.

3. Блок розпаковки операндів

Схема реалізації блоку розпаковки операндів приведена на рис. 4.

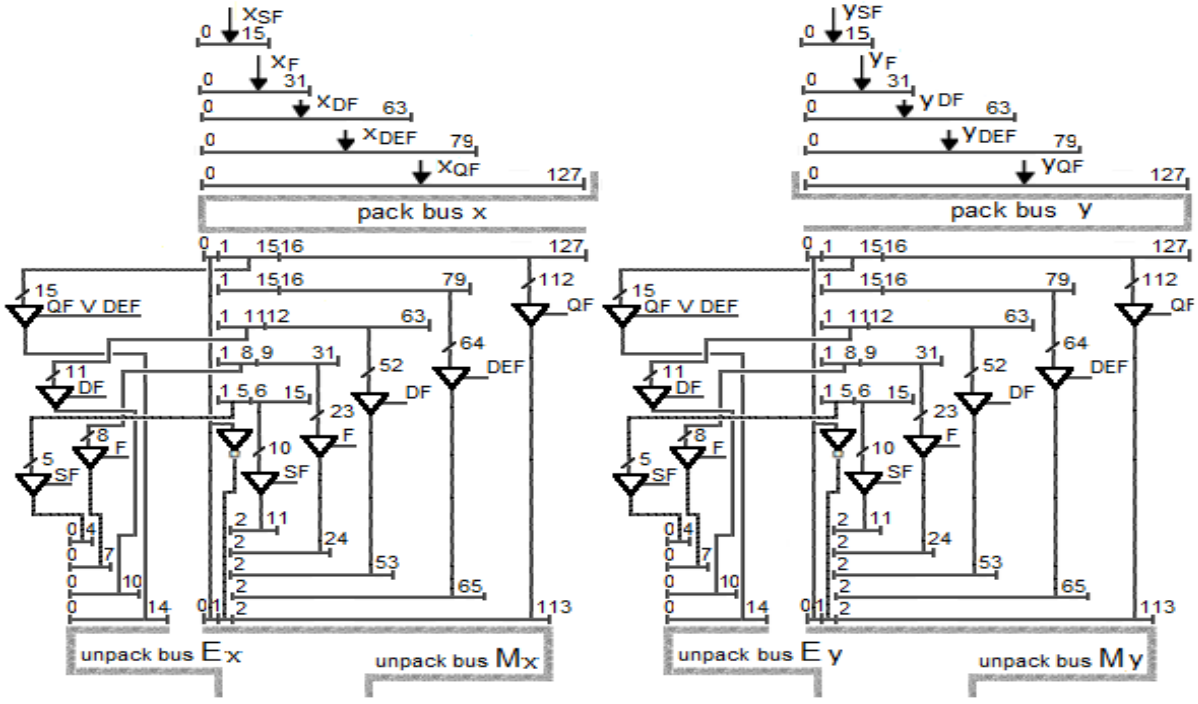

Рис. 4 Функціональна схема блоку розпаковки операндів

Основу блоку розпаковки операндів складають дві вхідні 128-розрядні шини упакованих операндів: pack bus x та pack bus y та чотири вихідні шини розпакованих операндів: 114-розрядні шини мантис операндів *unpack bus Mx* та *unpack bus My*, а також 15-розрядні шини порядків операндів unpack bus Ex та unpack bus Ey. Незалежно від формату оброблюваних операндів x та y вони завжди, на початку виконання операції перемноження, поступають із блоку регістрів з плаваючою крапкою загального призначення в старшу частину вхідної шини блоку розпаковки операндів. Розпаковка операндів здійснюється шляхом виконання потрібних зв'язків між вхідними шинами упакованих операндів та вихідними шинами порядків і мантис блоку розпаковки. Для створення потрібних зв'язків, в залежності від оброблюваного формату використовуються буфери з трьома станами, що створюють конструктивне «або» на вихідних шинах блоку. Для запобігання відмови блоку регістрів з плаваючою крапкою загального призначення, при розробці блока керування реконфігурованого помножувача з плаваючою крапкою, потрібно забезпечити умову, що в кожний момент часу, в залежності від оброблюваного формату операндів, повинен бути відкритим тільки один з буферів, що поєднуються конструктивним «або» на вихідній шині блоку.

При розпаковці операндів в 0-ий розряд кожної з вихідних шин мантис з відповідної вхідної шини напряму заноситься знак операнда, а в 1-ий розряд цих же шин, за допомогою інверторів, із знаків операндів відновлюються приховані біти.

4. Блок нормалізації та округлення результату

Якщо в результаті виконання операцій в блоках обробки мантис та порядків блок керування перемножувачем з плаваючою крапкою виявив наступні ситуації: ознака *Zero* (ознака рівності нулю мантиси результату), *NaN* («не число»), ±∞ («нескінченність»), то блок керування зразу ж ініціює виконання операції пакування числа відповідного результату, пропускаючи роботу блоку нормалізації.

В іншому випадку відбувається нормалізація результату. Функціональна схема блоку нормалізації приведена на рис. 5.

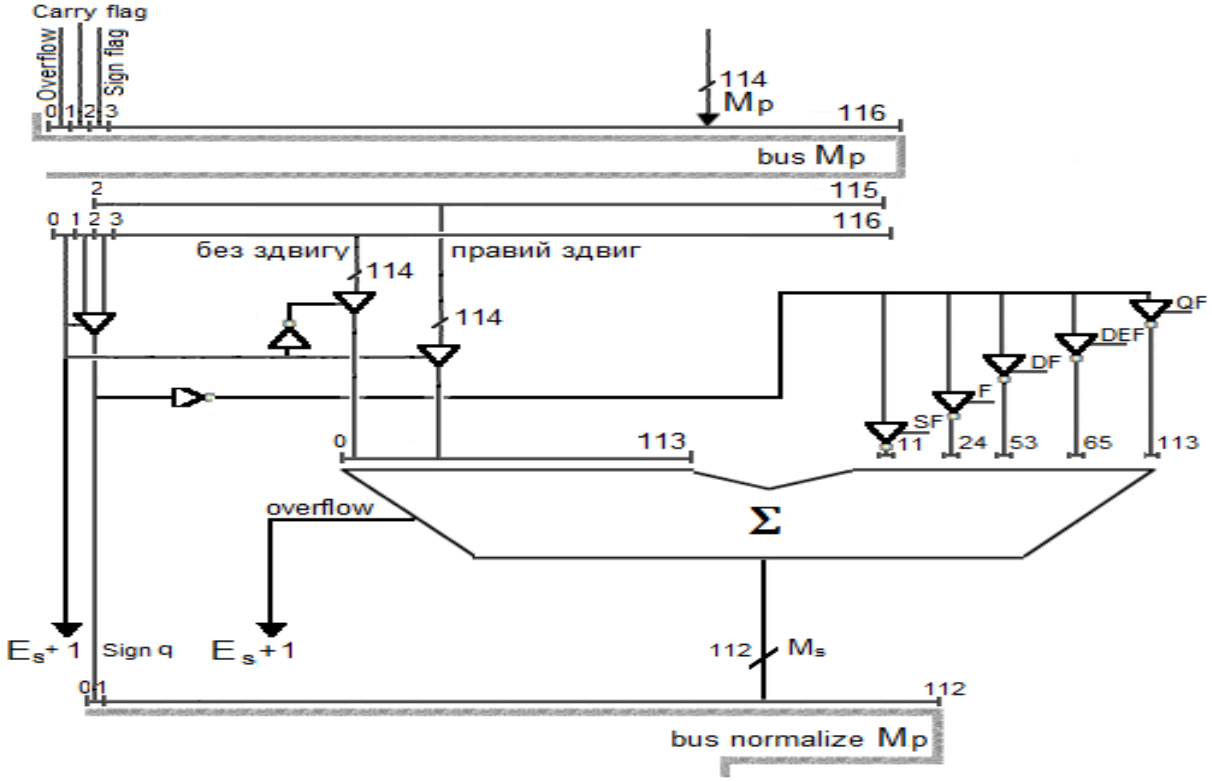

Рис. 5 Функціональна схема блоку нормалізації результату

Основу блоку нормалізації складають вхідна 117-розрядна шина bus Ms, що є вихідною шиною блоку обробки мантис і містить: в 0-му розряді сигнал *Overflow*, в 1-му розряді сигнал *Carry flag*, в 2-му розряді сигнал *Sign flag*, в 3 – 116 розрядах значення мантиси результату та 113-розрядна вихідна шина bus normalize Ms, що містить в 0-му розряді сигнал *Sign s*, а в розрядах 1 – 112 нормалізовану мантису без прихованого біта.

При перемноженні двох нормалізованих чисел з діапазону: $1 \le |x,y| < 2$ мантиса результату може знаходитися тільки в двох станах:

1. Мантиса результату є нормалізованою. При цьому мантиса результату повинна передаватися із вхідної шини на вихідну без зсуву з округленням у відкидаємому біті та видаленням прихованого біту.
2. Переповнення розрядної сітки. При цьому повинен виконуватися правий зсув мантиси на 1 розряд з видаленням прихованого біту та округленням у відкидаємому біті, а також в блок керування помножувачем з плаваючою крапкою повинен видаватися сигнал Es+1 для збільшення порядку результату на 1.

Робота блока нормалізації ґрунтується на організації безперебійної роботи конструктивного «або» на перших входах суматора. Для цього вивід з третього стану 115 – розрядного буферу, що виконує правий зсув мантиси результату, та 115 – розрядного буферу, що виконує передачу без зсуву, здійснюється відповідно, прямим та інверсним значенням одного й того ж сигналу Overflow (переповнення розрядної сітки). Така організація роботи схеми виключає одночасний вихід з третього стану обох буферів.

Знак результату передається з вхідної шини на вихідну без використання конструктивного «або». Для його передачі використовується двовхідний однорозрядний мультиплексор без третього стану, на керуючий вхід якого подається сигнал Overflow. При переповненні результату в якості його знаку передається Carry flag, в інших випадках – Sign flag.

Виконання округлення результату здійснюється шляхом подачі потрібного коду на другий вхід суматора в залежності від оброблюваної точності операндів та знаку результату.

Видалення прихованого біта забезпечується зв’язками між виходами суматора та вихідною шиною.

10. Висновки

В даній роботі описана реалізація помножувача з реконфігурованою структурою для виконання операцій з плаваючою крапкою. Розроблено моделюючу програму для дослідження швидкості та точності виконання частовживаної операції добутку чисел в арифметиці з плаваючою крапкою в розроблюваному помножувачі.

Помножувач реалізовано як набір комбінаційних схем, без використання елементів пам’яті, що не потребує мікропрограмного керування.

Виконана розробка буде корисною для подальшого вдосконалення помножувача з плаваючою крапкою та може бути використаною при побудові ядра мікропроцесора з суперскалярною архітектурою [3-6] в якості операційного пристрою.

Список літератури

1. IEEE 754: Standard for Binary Floating-Point Arithmetic [Електронний ресурс] / 3 квітень 2014. – URL: http://grouper.ieee.org/groups/754/.

2. C. R. Baugh and R. A. Wooley. A Two’s Complementpat Parallel Array Multiplication Algorithm. IEEE Transaction on Computers, C-22(12):1045–1047, December 1973.

3. Ajay D. Kshemkalyani, Mukesh Singhal «Deadlock detection in distributed systems», Distributed Computing Principles, Algorithms, and Systems, Cambridge University Press, 2008.ISBN 978-0-511-39341-9.

4. Луцький Г.М. та ін. «Розробка теоретичних основ побудови високопродуктивних комп'ютерних систем з динамічним розпаралелюванням обчислювальних процесів»- Закл. звіт по НДР № ДР 0213U004830. -Київ, 2013-165 с. – Депонований рукопис

5. K. Yeager. The mips r10000 superscalar microprocessor. IEEE Micro, 16(2):28–40, April 1996.

6. Яцун В.О., Долголенко О.М. Блок додавання та віднімання мантис з реконфігурованою структурою. Матеріали наукової конференції студентів, магістрантів та аспірантів «Інформатика та обчислювальна техніка – ІОТ-2016». Київ 25 – 27 квітня 2016, – с. 158-162 (http://fiot.kpi.ua/wp-content/uploads/2016/06/IOT-2016-OT.pdf).

УДК 004.274

СТОРОЖУК О. М.

БЛОЧНЕ РОЗВ'ЯЗАННЯ СИСТЕМ ЛІНІЙНИХ АЛГЕБРАЇЧНИХ РІВНЯНЬ ДЛЯ РЕКОНФІГУРОВНИХ ОБЧИСЛЮВАЛЬНИХ СИСТЕМ

Запропоновано модифікований спосіб розпаралелювання задач лінійної алгебри для реконфігуровних обчислювальних систем, що ґрунтується на блоковому LU-розкладі для розв'язання систем лінійних алгебраїчних рівнянь. Представлено результати моделювання способу для багаторазового обчислення лінійних алгебраїчних рівнянь великої розмірності, які обґрунтовують ефективність використання реконфігуровних обчислювальних систем для розв'язання задач лінійної алгебри.

A modified method of paralleling computing tasks of linear algebra for high-performance reconfigurable computing is proposed. The results, based on modeling LU-block schedule for repeated calculation of linear algebraic equations are presented. Experimental high efficiency reconfigurable computing in calculation of linear algebra problems is shown.

1. Вступ

У більшості сучасних систем комп'ютерного моделювання для вирішення різного роду завдань виникає необхідність багаторазового розв'язання систем лінійних алгебраїчних рівнянь (СЛАР), що потребує тривалих обчислень. Фундаментальні та прикладні розрахунки лінійної алгебри пов'язані з проведенням матричних обчислень, обсяг яких залежить від складності кінцево-елементної моделі, частоти дискретизації і необхідної точності. Вимоги до цих параметрів неухильно ростуть, і якщо на зорі обчислювальної техніки великими вважалися СЛАР, що складаються з півтора десятків рівнянь, то сьогодні, наприклад, для задач квантової механіки не є рідкістю рішення систем з десятками мільйонів невідомих [1].

Розробка спеціалізованих обчислювачів на основі універсальних процесорів не є оптимальним рішенням, оскільки така спеціалізація найчастіше обмежена ефективністю в якійсь конкретній задачі або проблемної області. Зі ще більшими труднощами пов'язане створення таких систем за допомогою проблемно-орієнтований процесорів (*Application Specific Integrated Circuit*, *ASIC*), так як тривалість і висока ціна розробки замовних схем виправдовують себе лише в разі їх великих тиражів для задач, які не потребують частої адаптації апаратної архітектури. Ці обмеження можуть бути подолані при використанні реконфігуровних обчислювальних систем (РОС) на базі динамічних програмованих логічних інтегральних схем (ПЛІС), які забезпечують гнучку апаратну архітектуру [2].

Динамічна часткова реконфігурація – це перепрограмування частини ПЛІС в режимі *RunTime*, коли інші її частини продовжують виконувати свої завдання. Розробник має можливість незалежно конфігурувати кожний обчислювальний вузол. Використання динамічної часткової реконфігурація є ефективне, оскільки це дозволяє значно зменшити непродуктивні часові витрати під час перепрограмування кристалу ПЛІС шляхом передавання часткового бітового потоку конфігураційних даних [3].

При використанні реконфігуровних систем основні обмеження визначаються тільки об'ємом внутрішніх ресурсів кристалу ПЛІС. Застосування сучасних ПЛІС з можливістю динамічної реконфігурації дає змогу змінювати модуль, котрий розташований на деякій частині пристрою, доки решта пристрою продовжує виконувати свою задачу. Різні апаратні модулі можуть розділяти в часі спільні фізичні ресурси, і апаратура може адаптуватись під програмні задачі "на льоту", або ж до частини задачі. Це дозволяє, прискорити обчислення та ефективно використовувати місце на платі [4], [5].

Для розв'язання задач лінійної алгебри в обчислювальних системах на базі ПЛІС найважливіше значення мають три фактори: загальний обсяг програмованої логіки, наявність апаратно реалізованих множників і достатньої кількості блочної пам'яті. Перші експериментальні використання реконфігуровних мікросхем почалися після досягнення ними порога еквівалентної ємності в 1 млн. вентилів [6]. Однак в той час через відсутність в кристалі помножувачів, доводилося або вибирати для реалізації ті алгоритми, в яких множення замінювалося послідовним додаванням, або розробляти власні версії апаратно-орієнтованих алгоритмів [7]. Після появи в ПЛІС апаратних блоків множення, стало можливим вирішувати задачі лінійної алгебри більш широкого діапазону. Реалізована в кристалі блочна статична пам'ять великої ємності дозволяє мінімізувати число звернень до зовнішньої динамічної пам'яті, що значним чином позначається на продуктивності обчислень. На відміну від *CPU*, де можливості розпаралелювання обмежені особливостями «жорсткої» архітектури кристалу, ПЛІС мають потенціал для створення реконфігуровних систем та демонструють кращу масштабованість і продуктивність в вирішенні задач лінійної алгебри. Таким чином виникає задача в розробці і застосуванні нових пристосованих методів паралельної реалізації матричних обчислень, відмінних від існуючих методів розпаралелювання, що використовуються в універсальних багатопроцесорних системах.

2. Особливості апаратної реалізації блочного LU – розкладу на ПЛІС

LU-розклад – це один із способів вирішення СЛАР виду *Ax = b*, при якому вихідна матриця А розбивається на добуток трикутних матриць *L* і *U* (де *L* та *U* є нижня та верхня трикутні матриці відповідно) і методом прямої і зворотної підстановки знаходиться вектор невідомих *x* [8].

$$A = LU = \begin{bmatrix} l_{11} & 0 & \dots & 0 \\ l_{21} & l_{22} & \dots & 0 \\ \dots & \dots & \dots & \dots \\ l_{n1} & l_{n2} & \dots & l_{nm} \end{bmatrix} \cdot \begin{bmatrix} u_{11} & u_{12} & \dots & u_{1n} \\ 0 & u_{22} & \dots & u_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & u_{nm} \end{bmatrix} \quad (1)$$

Декомпозиція єдина за умови, коли зафіксовані діагональні елементи однієї з матриць *L* або *U*. Це означає, що необхідно, щоб діагональні елементи нижньої чи верхньої трикутних матриць були рівні *1*. Якщо зафіксовані діагональні елементи матриці *L*, то факторизация називається розкладанням Дуліттла, а якщо зафіксовані діагональні елементи матриці *U*, то розкладанням Краута (рис. 1).

Таким чином, система рівнянь *Ax = b* зводиться до вигляду *LUx = b*. Обчислення елементів матриць-співмножників *L* і *U* виконується відповідно із формулами:

$$u_{11} = a_{11}, \quad u_{1j} = a_{1j}, \; l_{1j} = \frac{a_{j1}}{u_{11}},$$
$$j = 2,3, \; \dots, n;$$
$$u_{ii} = a_{ii} - \sum_{p=1}^{i-1} l_{ip} u_{pi}, i = 2,3,\dots,n, \quad (2)$$
$$u_{ij} = a_{ij} - \sum_{p=1}^{i-1} l_{ip} u_{pj}, i = 2,3,\dots,n;$$
$$l_{ji} = a_{ji} - \frac{\sum_{p=1}^{j-1} l_{jp} u_{pi}}{u_{ii}}, i = 2,3,\dots,n,$$
$$j = i+1, i+2,\dots,n.$$

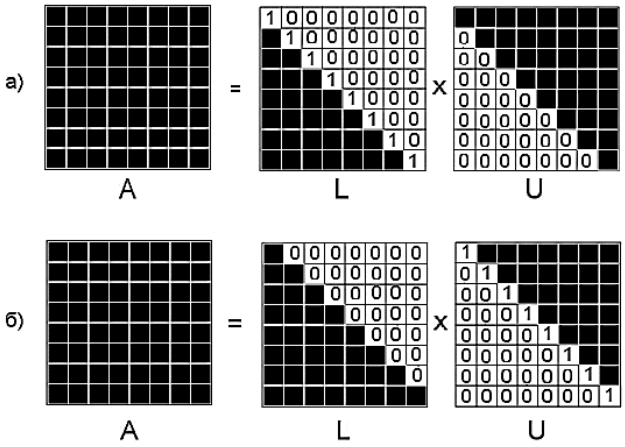

Рис. 1. Схема розкладу: а – Дулітла; б – Краута

Після отримання мультиплікативного представлення матриці, здійснюється знаходження вектору невідомих x_i шляхом послідовного розв'язання системи рівнянь $LUx=b$, яке проходить в дві стадії. На першій стадії, що є прямим ходом, знаходяться невідомі в системі $LU=b$.

$$y_i = \frac{b - \sum_{p=1}^{i-1} l_{ip} y_p}{l_{ii}}, i = 2,3,...,n, \quad (3)$$

На другій стадії розв'язується система рівнянь $Ux = y$

$$x_i = y_i - \sum_{p=i+1}^{n} u_{ip} x_p, i = 2,3,...,n, \quad (4)$$

LU-розклад має схожість з методом Гауса, але на відміну від нього дозволяє швидко вирішувати *СЛАР* з різними векторами в правій частині.

$$Ax = b_i, i = 1,2,...,m, m \quad (5)$$

Існує велика кількість варіантів *LU*-розкладу, орієнтованих на певні обчислювальні архітектури та способи зберігання матриці в пам'яті [9]. У нашому випадку реалізовано алгоритм *LU*-факторизації (рис. 2) щільної матриці, який використовується в стандартному пакетах реалізації алгоритмів лінійної алгебри *BLAS* (*Basic Linear Algebra Subprograms*), на основі чого основуються тести реальної продуктивності комп'ютерів *Linpack Benchmark* [10]:

```
double[] LUfactorization(double[,] matrix,
                         double[] rightPart, int n){
    double[,] lu = new double[n, n];
    double sum = 0;
    for (int i = 0; i < n; i++){
        for (int j = i; j < n; j++){
            sum = 0;
            for (int k = 0; k < i; k++)
                sum += lu[i, k] * lu[k, j];
            lu[i, j] = matrix[i, j] - sum;
        }
        for (int j = i + 1; j < n; j++){
            sum = 0;
            for (int k = 0; k < i; k++)
                sum += lu[j, k] * lu[k, i];
            lu[j, i] = (1 / lu[i, i]) *
            (matrix[j, i] - sum);
        }
    }
    double[] y = new double[n];
    for (int i = 0; i < n; i++){
        sum = 0;
        for (int k = 0; k < i; k++)
            sum += lu[i, k] * y[k];
        y[i] = rightPart[i] - sum;
    }
    double[] x = new double[n];
    for (int i = n - 1; i >= 0; i--){
        sum = 0;
        for (int k = i + 1; k < n; k++)
            sum += lu[i, k] * x[k];
        x[i] = (1 / lu[i, i]) * (y[i] - sum);
    }
    return x;
}
```

Рис. 2. Псевдокод алгоритму LU-факторизації

Наведений алгоритм полягає у виконанні вкладених циклів по змінних i, j, k, кожна з яких є одним з індексів двовимірного масиву коефіцієнтів СЛАР [11]. В *LU*-розкладі для забезпечення чисельної стійкості використовується вибір і перестановка ведучого елементу для виключення появи на головній діагоналі нулів і дуже маленьких чисел. Процес обчислення *LU*-розкладу вимагає обчислювати і зберігати елементи нижньої трикутної матриці. Ця обставина

вносить свої особливості в апаратну реалізацію даного алгоритму, що стосуються не тільки управління обробкою даних, але і різної інформаційної структури. На рис. 3. приведена обчислювальна структура, що відповідає базовому підграфу *LU*-розкладу.

Функціональні блоки всередині структури розподілені наступним чином. Блок *max* знаходить максимальний по модулю елемент, що надходить на його вхід і одночасно на вхід буферизованої в *FIFO* черги 1 і-ого рядка. Блок розподілу відповідно до алгоритму виконує ділення поточного елементу рядка $a_{i,k}$ на перший елемент цього ж рядка $a_{k,k}$. Результат ділення $m_{i,k}$, що представляє остаточно сформований елемент $a_{i,k}$ розкладеної матриці, запам'ятовується в блоці пам'яті *RAM* і одночасно надходить через мультиплексор на вихід для подальшої передачі результатів розкладу. Блок множення виконує операцію нормування – множення поточного елемента $a_{k,j}$ на нормувальний коефіцієнт $m_{i,k}$. Блок віднімання віднімає із поточного елемента $a_{i,j}$ результат нормування $m_{i,k} * a_{k,j}$

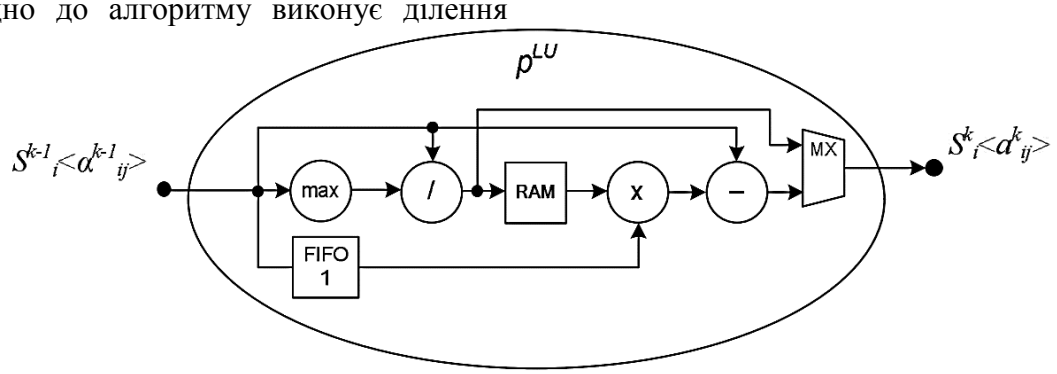

Рис. 3. Обчислювальна структура LU-розкладу

Елементи вихідного рядка *i*, розподілені таким чином, що перший з них належить першому елементу стовпчика нижньо-трикутної підматриці *L*, а всі наступні є елементами першого рядка верхньо-трикутної підматриці *U*. Таким чином, результатом роботи алгоритму на кожній ітерації *k* буде рядок матриці *U* (ведучий рядок *i* для ітерації *k+1*), стовбець матриці *L* і перелічені елементи квадратної підматриці.

Відповідно до наведеного методу була розроблена прикладна програма на мові високого рівня *C*, що реалізує рішення задачі *LU*-розкладу на мультипроцесорній реконфігуровані обчислювальній системі РОС на ПЛІС, що наведена на рис. 4.

Розроблена реконфігуровна система основана на архітектура із загальним комунікаційним середовищем «*Master-Slave*» («Головний» процесор – «Підлеглий» процесор) Дана система містить в собі спосіб управління, де головний (*Master*) процесор виконує функції управління системою та контроль поведінки підлеглих процесорів. Вона містить в основі програмовані процесорні ядра *Nios II*. Обчислення блоків матриці відбувається у програмному режимі під управлінням головного процесору *Nios II Master*. Обчислювальні вузли поєднуються загальним комунікаційним середовищем, а саме, загальною шиною.

Всі процесори підключені до спільної пам’яті через системну шину, для забезпечення безконфліктного доступу до загального ресурсу застосовується система арбітражу. Запис проміжних результатів відбувається через загальну шину в відповідності із алгоритм запису даних у пам’ять. Процесор, що в результаті реконфігурації, підключається до системної шини через систему арбітражу, генерує сигнали вимоги доступу r_i, який поступає на вхід арбітра, якщо шина вільна арбітр видає сигнал дозволу доступу q_i.

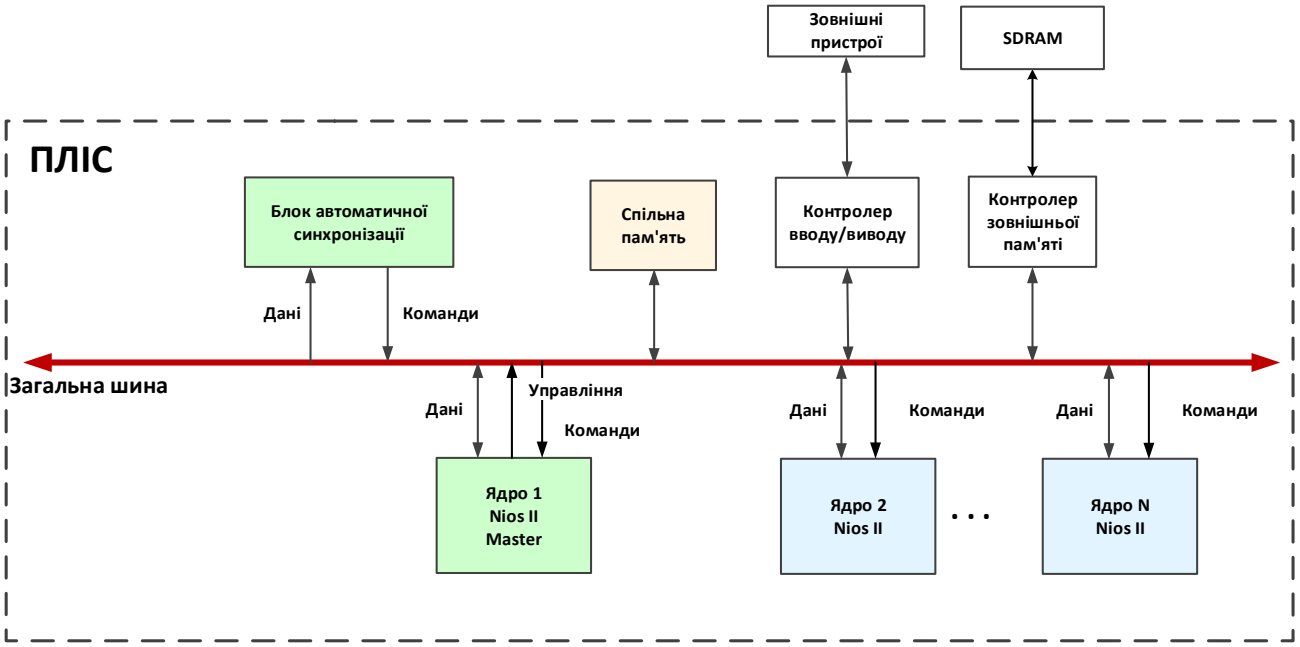

Рис. 4. Архітектура реконфігуровної обчислювальної систем-на-кристалі

Процесор, отримавши доступ до системної шини, розпочинає процедуру ініціалізації та отримання даних для виконання обчислень.

Модифікований алгоритм виконується на основі спеціалізованого модифікованого циклу запису даних, на протязі якого процесор видає на шину адреси адресу поточного блоку даних, адреса фіксується в інтерфейсі пам'яті в спеціальному регістрі адреси, далі процесор видає на шину даних масив слів, які за послідовністю сигналів процесора *w* (*write*) записуються в пам'ять. Далі процесор отримує від інтерфейсу пам'яті сигнали зворотного зв'язку *rd* (*ready*), що визначає закінчення операції запису інформації в пам'ять.

Під час звернення до загального системного ресурсу з боку активних пристроїв виникають так звані конфліктні ситуації, для вирішення яких в системі застосований централізований блок автоматичної синхронізації. Всі пристрої системи, що вимагають доступ до системної шини формують управляючий сигнал r_i, який надходить на входи блоку. У функції блоку входить перевірка зайнятості системної шини, низький рівень управляючого сигналу на шині визначає, що шина зайнята, та високий рівень сигналу – вільна. Якщо системна шина не зайнята, першому у черзі процесору надається доступ, при цьому арбітр формує сигнал зайнятості на шині, та сигнал надання доступу q_i, який надходить на управляючі входи відповідного процесора.

3. Моделювання модифікованого способу блочного LU-розкладу на ПЛІС

Обчислювальні експерименти були проведені на науковому стенді із вбудованою *ПЛІС* компанії *Altera, Cyclone II EP2C35F672C6*, що містить 33216 логічних елементів, 33216 комбінаційних функціоналів та 33216 логічних регістрів на кристалі. Загальна кількість внутрішньої пам'яті на чипі (*On-Chip Memory*) становить 483840 біт, що становить близько 59 Кбайт. На стенді вбудовано *8* Мб пам'яті *SDRAM*, *512* Кб пам'яті *SRAM,* 1 Мбайт пам'яті *Flash*, та інші інтерфейси. Підтримувана адресація зовнішньої пам'яті до 2 Гбайт.

Для розробки обчислювачів системи були обрані програмовані ядра типу *Nios II/s (Small core size),* так як вони є оптимальним рішенням, оскільки займають не значну кількість логічних елементів в кристалі (в порівнянні із ядром *Nios II/f*), а саме до 1400 *LEs (Logical Elements)*, що становить всього 4% від всього кристалу *ПЛІС*. І при цьому забезпечують значну продуктивність – 0,74 *DMIPS/MHz*, при частоті роботи ядра 165 *MHz*, максимальна продуктивність становитиме 127 *DMIPS (Dhrystone MIPS)*.

Час виконання задачі (матриці порядку $n = 1 \cdot 10^3$) на обчислювальній структурі, що складається з 6 обчислювальних блоків

(ядер) (одна ПЛІС) склало 32,1с. Програмна реалізація *LU*-розкладу матриці тієї ж розмірності на персональному комп'ютері (ПК) (*Intel Core i5*-4690, 3.5 ГГц, 8 Гбайт ОЗУ) показало час 5,7 с.

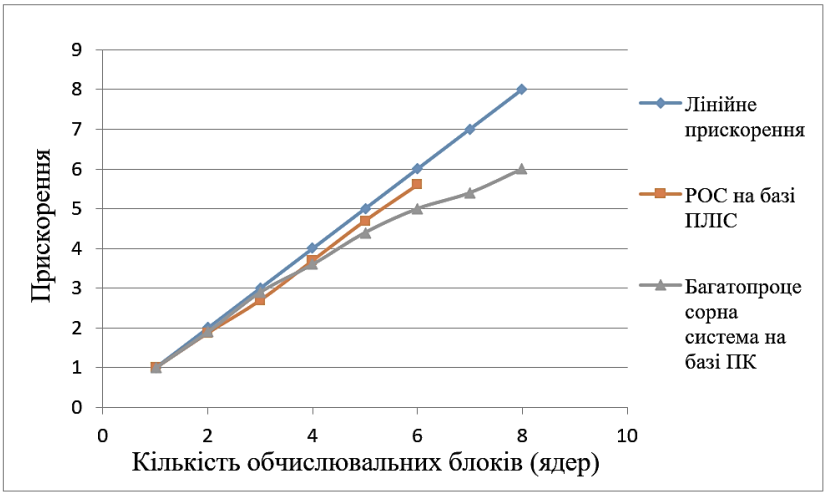

Рис. 5. Залежність прискорення LU-розкладу від кількості обчислювальних блоків на ПЛІС та ядер в ПК

Залежність прискорення від числа задіяних обчислювальних блоків сконфігурованих на ПЛІС для РОС, а також від числа процесорів в багатопроцесорній системі показано на рис. 5, де прискорення розраховується як $K_{Пр}=(T_1 - T_N)/N$, де N – кількість обчислювальних блоків (ядер), а T_1 та T_N час обчислення на одному та N ядрах відповідно.

Наведені графіки, демонструють практично лінійне зростання прискорення на РОС при фіксованому розмірі задачі, та погіршення прискорення в багатопроцесорній системі на базі ПК. Відсутність даних прискорення для 7 та 8 обчислювальних блоків на рис. 5, спричинено недостатність вбудованої пам'яті для розміщення в ній даної кількості програмованих ядер в науковому стенді *Cyclone II*, хоча тенденція графіку прискорення для меншої кількості програмованих ядер на ПЛІС показує практично лінійне зростання. Важливо відзначити, що досягнуті показники залежать тільки від внутрішніх властивостей обчислювальної системи (латентність, кількість обчислювальних блоків), пов'язаних з розмірністю завдання.

В той час як ефективність масштабування задачі в багатопроцесорній системі залежить як від розмірності задачі, так і інших чинників: конфігурація розбиття, розмір порції даних, топологія комунікаційної мережі і так далі. Ефективність *LU*-розкладу в РОС і в багатопроцесорному ПК наведені на графіках, зображених на рис. 6, де ефективність розраховується як $K_{еф} = K_{Пр} / N$, де $K_{Пр}$ – коефіцієнт прискорення, а N – кількість обчислювальних блоків (ядер).

Наведені результати показують, що середня ефективність РОС у вирішенні даної завдання складає 0,97. При збільшенні обчислювального ресурсу підвищення ефективності LU-розкладу на РОС в порівнянні з багатоядерним ПК в середньому склало 14%. Як було зазначено вище, відсутність даних ефективності для 7 та 8 блоків для обчислень на ПЛІС, на рис. 6, спричинено недостатність вбудованої пам'яті для розміщення в ній даної кількості програмованих ядер в науковому стенді *Cyclone II,* хоча з графіка видно що вже починаючи від 4 і більше програмованих ядер, обчислення в РОС показує кращу ефективність в порівнянні з багатопроцесорною системою на базі жорсткої архітектури ПК.

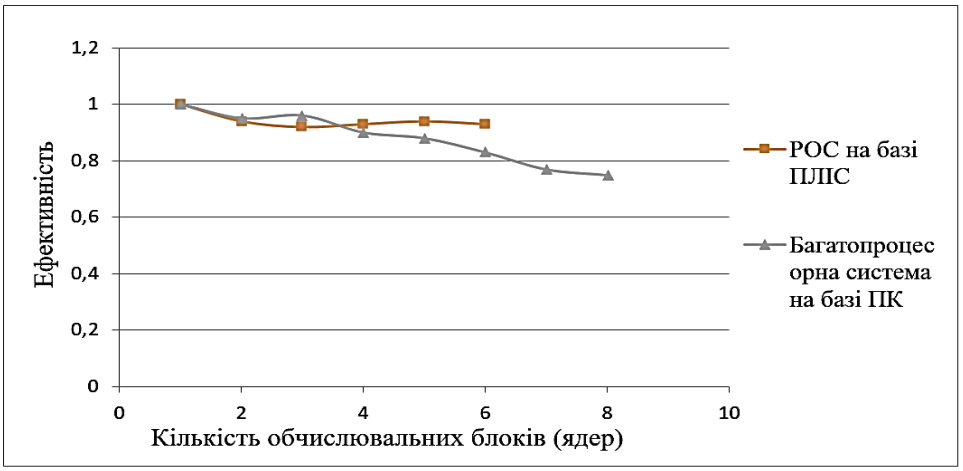

Рис. 6. Залежність ефективності LU-розкладу від кількості задіяних обчислювальних блоків на ПЛІС та ядер в ПК

4. Висновки

Використання реконфігуровних обчислювальних систем з адаптивною до вимог задач архітектурою створює передумови для підвищення ефективності розв'язання задач, в яких виникає необхідність багатократного вирішення систем лінійних алгебраїчних рівнянь великої розмірності. Застосування програмованих логічних інтегральних схем, як елементної бази для створення відповідного середовища, сприяє підвищенню швидкодії обчислень, зменшенню споживної потужності, розмірів та вартості обчислювальної системи.

Проведені в роботі експерименти показали, що можливість прискорення обробки даних за рахунок коректного розташування блоків і їх сегментації дозволяє реалізувати найбільш ефективні обчислювальні структури на ПЛІС для розпаралелювання задач лінійної алгебри.

Дослідження показали прискорення обробки даних під час багаторазових обчислень СЛАР для двовимірних і тривимірних обчислювальних структур реалізованих на ПЛІС. За результатами моделювання отримано середнє значення ефективності обчислень близько 97%, що на 14% більше в порівнянні з організацією обчислень на мультипроцесорній системі.

Ефективність використання запропонованого способу блочного *LU*-розкладу в реконфігуровних обчислювальних системах на базі ПЛІС значно вища в порівнянні з мультипроцесорними системами з жорсткою архітектурою. Ефективність обробки даних в реконфігуровних обчислювальних системах майже не залежить від масштабування обчислювального середовища, що дозволяє спростити масштабування обчислювальних систем залежно від розмірності вирішуваних задач.

Використання динамічної часткової реконфігурації, потребує коректив в підходах до проектування, що призводить до необхідності розробки та пошуку нових методів та модифікації існуючих алгоритмів розв'язання специфічних задач та методів і засобів обробки даних. Це може бути перспективним напрямом подальших досліджень в області підвищення ефективності функціонування реконфігуровних обчислювальних систем.

Список літератури

1. Жуков І. А. Обчислювальна система для розв'язку нечітких СЛАР / І. А. Жуков,vI. А. Клименко // Проблеми інформатизації та управління : зб. наук. праць. – К. : НАУ, 2011. – Вип. 3 (35). – С. 34 – 43.

2. Клименко І. А. Оптимізація реконфігурації в динамічно реконфігурованих обчислювальних системах / І. А. Клименко // Вісник НТУУ «КПІ». Інформатика, управління та обчислювальна техніка : зб. наук. праць. – К. : Век+, 2015. – № 63. – С. 93 – 100.

3. Compton K. and Hauck S. Reconfigurable Computing: A Survey of Systems and Software // ACM Computing Surveys ,vol. 34, no. 2, pp. 171–210, June 2002.

4. Xilinx Inc. Press Release: ISR and Xilinx Roll Out Ready-to-Wear SDR. Xilinx Inc., San Jose, CA., 2006, www.fpga journal.com.

5. Programmable Logic Design Line. Xilinx honored for enabling technology in the ALICE experiment at CERN. Xilinx Inc., San Jose, CA., 2008, http://www.pldesignline.com/news/207101017.

6. Сергиенко А. М. Процессор для безошибочного вычисления обратных матриц / А. М. Сергиенко, В. Л. Лепеха, Т. М. Лесик. // Міжнародна конференція "Високопродуктивні обчислення 2012". – 2012. – С. 305–307.

7. Стрельников О. И. Разработка и исследование аппаратурно-ориентированных алгоритмов для нахождения собственных значений матриц : дис. канд. техн. наук / Стрельников О. И. – Волгоград, 2002. – 167 с.

8. Nicolas J. H. Accuracy and Stability of Numerical Algorithms / Highman Nicolas. – Philadelphia: SIAM, 1961. – 680 p.

9. Ортега Д. Введение в параллельные и векторные методы решения линейных систем / Дж Ортега., 1991. – 376 с. – (Мир).

10. Dongarra J. LINPACK Users' Guide / Dongarra J., Bunch J., Moler C. and Stewart G. W. // SIAM, Philadelphia, PA, 1979, p. 1.4.

11. Баркалов К. А. Методы параллельных вычислений / К. А. Баркалов. – Н. Новгород: Нижегородского госуниверситета им. Н. И. Лобачевского, 2011. – 124 с.

УДК 004.052.42

ФЕДОТОВ М.Ф.

МЕТОД ІДЕНТИФІКАЦІЇ ВІДДАЛЕНИХ АБОНЕНТІВ НА ОСНОВІ КОНЦЕПЦІЇ “НУЛЬОВИХ ЗНАНЬ”

В статті представлено метод реалізації теоретично строгої ідентифікації віддалених користувачів або термінальних пристроїв багатокористувацьких систем, що реалізує концепцію “нульових знань”. Метод має за основу використання математичних незворотних перетворень теорії чисел. Визначальна особливість методу полягає в використанні одного сеансу пересилки ідентифікуючої інформації між користувачем та системою. Це дозволяє суттєво прискорити процес ідентифікації. Передбачені методом процедури реєстрації користувача та його ідентифікації ілюстровані числовим прикладом. За результатами експериментальних досліджень проведене порівняння запропонованого методу та відомих.

In article the new method for implementation of theoretical strong identification of remote abonents or tample-resistant devices of multiuser systems, based on zero-knowledge conception is presented. The need for efficient remote users identification procedure is hence explained. The mathematic background of proposed method consist of using the number theory irreversible transformation. The main peculiarities of proposed method consist of that identification process only takes a single cycle of information exchanges between the user and the system and hence reduces the overhead of the authentication process while minimizing the danger of malicious third parties intervening during this process. Apart from it allows to speed up of identification process for software and hardware implementation. The technology of mathematical transformations whose are provided by proposed method are set forth clearly. A numerical example for designed procedures of user registration and user is given. It has been shown that

Ключові слова: багатокористувацькі системи, ідентифікація віддалених користувачів, методи строгої ідентифікації користувачів, концепція ідентифікації “нульових знань”, модулярне експоненціювання.

1. Вступ

Інтегровані системи зберігання та обробки даних з колективним доступом відіграють зростаючу роль в глобальних процесах інформаційної інтеграції. Така інтеграція дозволяє підвищити ефективність комп’ютерної обробки даних за рахунок надання доступу до інформаційних, програмних та обчислювальних ресурсів широкому колу користувачів.

Розвиток інтегрованих систем обробки інформації значною мірою залежить від ефективності реалізації в них функцій захисту інформації та розподілення прав доступу. Ключова роль у вирішенні цієї проблеми належить засобам ідентифікації абонентів. Розширення використання багатокористувацьких систем пов’язане зі зростанням ризиків несанкціонованого доступу до їх інформаційних та обчислювальних ресурсів. Це зумовлено, з однієї сторони, ростом технічних можливостей для реалізації несанкціонованого доступу, а з іншого – збільшенням потенційних вигод з цього. Факторами, що підвищують ризик несанкціонованого доступу до ресурсів інтегрованих систем обробки інформації є розширення використання потенційно відкритих для стороннього впливу бездротових систем передачі даних комп’ютерних мереж, підвищення продуктивності обчислювальних засобів, що використовуються для несанкціонованого доступу, збільшення кількості віддалений користувачів, і, відповідно зменшення обчислювальних ресурсів, які використовуються для захисту від несанкціонованого доступу.

За цих умов необхідністю є адекватне вдосконалення всього арсеналу засобів, які виключають можливість несанкціонованого доступу до ресурсів інтегрованих систем, в тому числі методів та засобів ідентифікації їх віддалених абонентів.

Таким чином, задача підвищення ефективності ідентифікації абонентів багатокористувацьких систем є важливою і актуальною для сучасного етапу розвитку комп'ютерних та мережевих технологій.

2. Аналіз відомих технологій ідентифікації віддалених абонентів

Базовими критеріями ефективності будь-якої системи захисту є рівень захищеності, що досягається при її використанні та об'єм ресурсів, що застосовується для реалізації функцій захисту. Відповідно, в процесі розробки будь-якої системи захисту даних, в тому числі і засобів ідентифікації віддалених абонентів, потрібно досягати компромісу між рівнем захищеності та продуктивністю реалізації функцій захисту.

Складність проблеми визначається неможливістю побудови адекватної формальної моделі дій сторони, що намагається реалізувати незаконний доступ до ресурсів системи. В першому наближенні процедура ідентифікації має задовольняти таким вимогам [1]:

1) Організація зберігання ідентифікуючої інформації має бути такою, щоб одна її частина зберігалася у абонента, а друга – в системі і кожна з цих частин не була б самодостатньою для доступу до ресурсів системи.

2) Ідентифікаційна посилка абонента при кожному сеансі підключення до системи має змінюватися.

3) Об'єм секретної інформації, що зберігається в системі і використовується для ідентифікації має бути якомога меншим з тим, щоб надати можливість збереження такої інформації в спеціальній захищеній на апаратному рівні пам'яті.

Всі сучасні протоколи ідентифікації абонентів розділяють на два класи: з використанням паролів, що перевіряються системою шляхом порівняння ("слабка" ідентифікація) та на основі теоретичної концепції "нульових знань" ("строга" ідентифікація) [2].

В основі більшості протоколів ідентифікації віддалених абонентів лежить теоретична концепція "нульових знань". Сутність цієї концепції полягає в тому, що для доведення своєї автентичності абонент має неявним чином виявити знання певної інформації, якою система не володіє, але може перевірити її наявність у абонента.

При цьому в системі не зберігається ніякої секретної інформації, яка дозволяє відновити ідентифікаційні дані абонента, що пояснює походження назви концепції "нульових знань". Важливим є те, що при кожному зверненні до системи абонентом генерується нова ідентифікуюча інформація.

Таким чином, концепція нульових знань в теоретичному плані найбільш повною мірою відповідає сформульованим вище вимогам щодо системи ідентифікації абонентів. В сучасних умовах і у найближчій перспективі потрібний для практики рівень надійності ідентифікації може бути забезпечений лише методами, що спираються на концепцію "нульових знань".

Концепція "нульових знань" передбачає використання незворотних математичних перетворень. Це означає, що існує алгоритм перетворення в прямому напрямку, але принципово неможливим є аналітичне віднаходження алгоритму зворотного перетворення. В більшості існуючих схем ідентифікації на основі концепції "нульових знань" для реалізації такого перетворення використовуються аналітично нерозв'язувані задачі теорії чисел, зокрема відома задача дискретного логарифмування.

Найбільш відомими з схем ідентифікації цього класу є FFSIS (Feige Fiat Shamir Identification Scheme) [2], методи Шнора (Schnorr) та Гіллоу-Квіскватера (Guillou-Quisquater) [3]. Базовими обчислювальними операціями для FFSIS є $A^2 \cdot B \bmod m$, а для методів Шнора і Гіллоу-Квіскватера - $A^e \cdot B^v \bmod m$.

З викладеного слідує, що базовою обчислювальною операцією більшості схем строгої ідентифікації віддалених абонентів є модулярне експоненціювання над числами, довжина яких значно перевищує розрядність процесору. В умовах стійкої тенденції до зростання розрядності чисел, обчислювальна складність реалізації вказаного типу операцій

збільшується експоненційно, випереджаючи темпи зростання продуктивності комп'ютерних систем.

Опубліковано [4] результати спроб використання при реалізації концепції "нульових знань" в якості незворотного булевих функціональних перетворень. Таке рішення дозволяє на порядки прискорити процедуру ідентифікації віддалених абонентів. Недоліками такого рішення є суттєве обмеження на кількість сеансів ідентифікації, складність процедури генерації незворотного та багатозначного булевого перетворення, значний об'єм пам'яті для зберігання в системі таблиць перетворень для кожного з абонентів. Суттєвим моментом є те, що не проведені об'ємні та всебічні дослідження рівня захищеності. Тому цей метод не дійшов до рівня практичного застосування в діючих протоколах ідентифікації.

На основі проведених літературних джерел можна зробити наступні висновки. З теоретичної точки зору найбільш надійна ідентифікація віддаленого користувача досягається в рамках реалізації концепції "нульових знань".

Існуючі методи реалізації вказаної концепції мають за математичну основу аналітично нерозв'язну задачу дискретного логарифмування. Відповідно, базовими обчислювальними операціями для відомих методів виступають мультиплікативні операції модулярної арифметики. Для зменшення обчислювальної складності реалізації цих методів в відомих методах застосовано певні спрощення, зокрема використання операції модулярного піднесення до квадрату та чисел з меншою розрядністю. Ці спрощення компенсуються використанням декількох (від 3-х до 20) сеансів обміну даними між користувачем та системою, що суттєво уповільнює ідентифікацію користувачів.

В сучасних умовах практично всі сервери систем віддаленого надання користувачам доступу до інформаційних та обчислювальних ресурсів обладнані криптопроцесорами, які здатні з високою швидкістю виконувати мультиплікативні операції модулярної арифметики над числами, розрядність яких становить до 4096. Разом з тим, для обчислювальної платформи користувача, що не має крипто процесора час виконання мультиплікативних операцій модулярної арифметики суттєво впливає на швидкість ідентифікації. Таким чином, в сучасних умовах витрати часу на виконання обчислень на сервері системи, пов'язаних з процесом ідентифікації, стають менш критичним в порівнянні з часом, що витрачається на багатокроковий обмін даними. Відповідно, важливим резервом прискорення процесів ідентифікації користувачів в умовах багатократного зростання їх кількості є зменшення використання ліній передачі даних.

Ціль досліджень полягає в прискоренні процедури криптографічно строгої ідентифікації віддалених користувачів в рамках концепції "нульових знань" за рахунок зменшення кількості сеансів обміну даними між системою та користувачем.

3. Метод ідентифікації на основі властивостей циклічності модулярних операцій

Для підвищення ефективності ідентифікації віддалених абонентів за рахунок зменшення кількості сеансів обміну інформацією між користувачем та системою пропонується метод ідентифікації, що має за математичну основу реалізації теоретичної концепції "нульових знань" незворотні перетворення теорії чисел.

В основі запропонованого методу ідентифікації віддалених користувачів покладено наступні теоретичні положення теорії чисел.

Якщо модуль M утворюється у вигляді добутку двох простих чисел p і q: $M=p\cdot q$, то функція Ейлера φ(M) визначається у вигляді $\varphi(M) = (p-1)\cdot(q-1)$. За умови, що найбільший спільний подільник (НСП) A та M дорівнює одиниці, тобто НСП$(A,M)=1$, то, згідно з узагальненням Ейлера малої теореми Ферма [4] : $A^{\varphi(M)} \bmod M = 1$. Наприклад, якщо $p= 19$, а $q = 13$, то модуль $M=p\cdot q = 19\cdot 13 = 247$, функція Ейлера $\varphi(M) = (p-1)\cdot(q-1) = 216$ і для будь-якого A, що не ділиться на $p=19$ або $q=13$ $A^{216} \bmod 247 = 1$, зокрема $225^{216} \bmod 247 = 1$.

Розроблений метод, що реалізує теоретичну концепцію "нульових знань" строгої ідентифікації віддалених користувачів, як і

інші методи, передбачає процедури, що виконуються при реєстрації користувача в системі та процедури, що реалізуються безпосередньо в кожному циклі ідентифікації.
Процедура реєстрації користувача складається з наступної послідовності дій:
1) Користувач довільним чином вибирає два простих числа p і q. Бажано, щоб вибір пари простих p і q виконувався таким чином, щоб числа p-1 та q-1 мали якомога більше подільників. Формується модуль M як добуток вибраної пари простих чисел: $M=p\cdot q$. Обчислюється число $\varphi = (p-1)\cdot(q-1)$, що зберігаються користувачем в секреті. Зберігається також множина ϑ його можливих подільників.
2) По запиту користувача система пересилає йому свій відкритий закриваючий ключ $K_з$, який надає змогу шифрувати реєстраційні дані, що передаються в систему кожним із користувачів. В якості алгоритму несиметричного шифрування використовується алгоритм з відкритим ключем типу RSA. Відкриваючий ключ K_0 тримається системою в секреті.
3) Отримане значення модуля M шифрується відкритим ключем $K_з$ системи та пересилається в систему в якості відкритого ключа користувача.
4) З використанням секретного відкриваючого ключа K_0 система відновлює відіслане користувачем значення модуля M і зберігає його.
Передбачена розробленим методом процедура циклу ідентифікації полягає в виконанні наступної послідовності дій:
1) Користувачем генерується випадкове число A.
2) Виконується перевірка чи ділиться число A на p чи q . Якщо $A \bmod p = 0$ або $A \bmod q$, то перехід на повторне виконання п.1.
3) З використанням множини ϑ користувачем виконується розкладення числа φ на два співмножника v та w: $\varphi = v\cdot w$.
4) Виконується обчислення першої компоненти сеансового паролю $P = A^v \bmod M$. В якості другої компоненти сеансового пароля слугує число w.
5) Обидві компоненти сеансового паролю P та w шифруються системним відкритим ключем K_3 та відсилаються користувачем в систему.
6) Система з використанням закритого ключа K_0 розшифровує ідентифікуючую посилку користувача, відновлюючи обидві компоненти сеансового паролю P та w.
7) Система обчислює $Z = P^w \bmod M$ і порівнює отриманий результат з одиницею. Якщо $Z = 1$, то вважається, що ідентифікація користувача виконана успішно і останній отримує доступ до ресурсів системи.
Функціонування запропонованого методу може бути ілюстровано наступним прикладом. Згідно з описаною вище процедурою реєстрації, користувач довільним чином вибирає два простих числа p і q такі, щоб значення p-1 і q-1 мали якомога більше подільників. Наприклад, при виборі простого $p=19$ значення p-1=18 має чотири подільники 2, 3, 6 і 9, а при виборі простого q=17 значення q-1=16 має три подільники*: 2,* 4, 8. Обчислюється число $\varphi = (p-1)\cdot(q-1) = 18\cdot16 = 288$, що зберігається в секреті. Зберігається також множина ϑ його можливих подільників.
Користувач обчислює значення модуля $M=p\cdot q = 19\cdot17 = 323$. Обчислене значення в зашифрованому вигляді пересилається в систему і являє собою відкритий ключ користувача.
Для виконання циклу ідентифікації користувач, згідно п.1 описаної процедури генерує випадкове число, наприклад, A= 255. В рамках п.2 виконується перевірка того, що вибране число не ділиться на одне з двох чисел p і q. Оскільки $255 \bmod 19 = 8 \neq 0$ але $255 \bmod 17 = 0$, тобто згенероване число A ділиться на q=17, то реалізується перехід на повторне виконання п.1 запропонованої процедури.
При повторному виконанні п.1 користувач генерує випадкове число A= 100 Наступним п.2 виконується перевірка $100 \bmod 19 = 5 \neq 0$ або $100 \bmod 17 = 15 \neq 0$.
В рамках п.3 запропонованої процедури користувачем виконується розкладення числа φ=288 на два співмножника v та w: наприклад *v=32* та *w=9.* Виконується обчислення першої компоненти сеансового паролю $P = A^v \bmod M = 100^{32} \bmod 323 = 256$. Друга компонента сеансового паролю w=9. Пара чисел P = 256 та w=9 шифруються відкритим системним ключем K_3 та передаються в систему. Остання розшифровує отримане повідомлення з

використанням закритого ключа K_0 , відновлюючи значення $P = 256$ та $w=9$. У відповідності до п.7 описаної вище процедури ідентифікації система обчислює значення $Z= P^w \bmod M \;\; Z = 256^9 \bmod M \;\; 323 = 1$. В силу того, що обчислене значення Z дорівнює одиниці, що підтверджує ідентичність користувача. ідентифікація вважається виконаною успішно.

4. Оцінка ефективності

Основними показниками ефективності процедури ідентифікації , як і будь-якого механізму криптографічного захисту інформації є рівень захищеності та швидкість реалізації функцій захисту.

В теоретичному плані запропонований метод ідентифікації віддалених користувачів цілком відповідає концепції “нульових знань” в силу того, що:

- сеансові паролі змінюються в кожному циклі ідентифікації;
- системі надано механізм перевірки правильності сеансових паролів користувачів, проте сама система не може генерувати такі паролі.

Для того, щоб система могла генерувати коректний сеансовий пароль у вигляді пари чисел P та w таких, щоб $P^w \bmod M = 1$ їй потрібно фактично відновити значення простих співмножників модуля M - простих чисел p та q, таких, що $M = p \cdot q$. Це класична задача [5] розкладення числа на прості співмножники, Вирішення такої задачі при розрядностях M більших за 1024, потребує ресурсів, об’єм яких в переважній більшості випадків виходить за рамки практичної доцільності навіть при використанні сучасних хмарних технологій [6].

Таким чином, при використанні запропонованого методу, система практично не здатна генерувати коректний сенсів пароль користувача. Відповідно, виключається можливість імітації звернення користувача до системи та використання інформації. що міститься в системі для генерації коректних сеансових паролів користувачів.

Для сторони, яка здійснює пасивний чи активний доступ до каналу передачі даних, підбір корректного сеансового пароля ускладнюється тим, що їй не відомий модуль M. Відповідно, для цієї сторони задача отримання можливості отримання незаконного доступу до ресурсів системи за рахунок підробки сеансових паролей користувачів практично не може бути реалізована.

Основна перевага розробленого методу ідентифікації віддалених користувачів полягає в використанні лише одного використання каналу передачі даних між системою та абонентом. Це дозволяє в сучасних умовах суттєво прискорити виконання процедури ідентифікації в порівнянні з відомими методами. Фактично, час потрібний на виконання ідентифікації визначається двома складовими: часом на реалізацію передбачених методом обчислень та часом, потрібним для обміну ідентифікаційною інформацію між системою та користувачем.

В сучасних умовах динамічного розвитку хмарних технологій і, відповідно, лавиноподібного зростання кількості користувачів інтегрованих систем надання інформаційних та обчислювальних ресурсів, питома вага часової складової пов’язаною з обміном даними має тенденцію до зростання. Основні чинники цього полягають в зростанні кількості користувачів, звернення яких до системи носить випадковий характер. Разом з тим, практично всі сучасні сервери обладнані спеціалізованими криптопроцесорами, які здатні швидко реалізувати операції модулярного експоненціювання над числами розрядністю 1024, 2048 та 4096. Зокрема, криптопроцесор моделі 6500 американської фірми Hi/fn виконує операцію модулярного експоненціювання на десятки наносекунд. Це має наслідком значне зменшення питомої ваги часових затрат на ідентифікацію, пов’язаних з виконанням відповідних обчислень.

В запропонованому методі найбільш ресурсоємкі операції модулярного експоненціювання виконуються як користувачем так і системою. Остання реально виконує ці операції на криптопроцесорі сервера системи і, відповідно, їх виконання не займає багато часу. Проте, в переважній своїй більшості, обчислювальні платформи користувачів не обладнані спеціалізованими криптопроцесорами. Відповідно, виконання операцій, передбачених п.3 та п.4 наведеної

вище процедури ідентифікації займають доволі багато часу. Проте, як видно з наведеної процедури, вказані операції можуть виконуватися заздалегідь і час їх виконання прямо не впливає на швидкість ідентифікації користувача.

Таким чином, використання в розробленому методі однієї пересилки надало змогу фактично виключити з сумарного часу проведення ідентифікації час, потрібний на обчислення, що виконує користувач. Саме ця відмінність запропонованого методу, як показали результати експериментальних досліджень, суттєвим чином впливає на час ідентифікації.

5. Висновки

В результаті проведених досліджень розроблено метод, що реалізує теоретичну концепцію "нульових знань" строгої ідентифікації віддалених користувачів інтегрованих систем надання інформаційних та обчислювальних ресурсів. Відмінність запропонованого методу полягає з використанням одного сеансу обміну даними між системою та користувачем, що дозволяє прискорити процес його ідентифікації. Математичною основою запропонованого методу є використання незворотних перетворень теорії чисел. Метод безпосередньо базується на властивостях узагальнення Ейлера малої теореми Ферма.

Проведений теоретичний аналіз рівня захищеності від спроб незаконного проникнення до ресурсів системи, що забезпечує запропонований метод, показав, тотожність задачі порушення захисту математичним задачам, розв'язання яких потребує обчислювальних ресурсів, об'єм яких знаходиться за межами практичної доцільності. Проведеними експериментальними дослідженнями показано, що розроблений метод забезпечує прискорення процесу ідентифікації віддалених користувачів в порівнянні з відомими методами, що базуються на теоретичній концепції "нульових знань".

Список літератури

1. Schneier B. Applied Cryptography. Protocols. Algorithms and Source codes in C. -Ed.John Wiley, 1996 - 758 pp.

2. Feige U. Zero knowledge proofs of identity / Feige U.,Fiat A.,Shamir A.// Journal of Cryptology.- v.1.- №.2.- 1988, pp.77-94.

3. Pourand G. A realistic security analysis of identification schemes based on combinatorial problems // European Transactions on Telecommunications.- V.8,-№.5.- 1997,- pp.471-480.

4. Markovskyy O. Fast subscriber identification based on the zero knowledge principle for multimedia content distribution/ O. Markovskyy, N. Bardis, N. Doukas // International Journal of Multimedia Intelligence and Security 2010 - Vol. 1,- pp.78-82.

5. Зенин О.С. Стандарт криптографической защиты AES./ Зенин О.С., Иванов М.А. - М.:Из-во Кудиц-Образ.-2002.- 174 с.

6. Elbirt A. An FPGA Implementation and Performance Evaluation of the AES Block Cipher Candidate Algorithm Finalists // Proceedings of The Third Advanced Encryption Standard Candidate Conference. NIST, Gaithersburg, MD,- 2000.- pp 13-27.

УДК 004.27

ШПАРТЬКО О. В.
КЛИМЕНКО І. А.

ОСОБЛИВОСТІ СУЧАСНОЇ МЕТОДОЛОГІЇ РОЗРОБКИ МІКРОПРОЦЕСОРНИХ СИСТЕМ

Досліджено методологію створення мікропроцесорних систем для обробки інформації, які базуються на використанні сучасних мікроконтролерів. Розглянуто питання структурного і програмного синтезу мікропроцесорних систем на базі сучасної елементної бази.

Researched the methodology of creatitg microprocessor systems for information processing based on the use of modern microcontrollers. The issue of structural synthesis software and microprocessor systems based on modern components.

1. Вступ

Протягом останніх років актуальною є тематика є використання мікроконтролерів для побудови систем обробки інформації. На сьогодні навіть найпростіші електронні пристрої обладнані мікроконтролером. А висока швидкодія і широкі функціональні можливості сучасних мікроконтролерів дозволяють створювати досить потужні системи для рішення завдань різної складності. Мікроконтролери застосовуються досить широко в якості вбудованих систем, починаючи від управління побутовою технікою та системами «*smart house»* і закінчуючи управлінням окремими технічними та технологічними процесами на виробництві. Виходячи з цього, найбільш розповсюдженою галуззю застосування мікроконтролерів є системи керування. Зростання складності розв’язуваних задач накладає певні вимоги до структури і можливостей систем керування, які стосуються забезпечення високої продуктивності, енергозбереження, відмовостійкості, живучості, адаптивності до класів розв’язуваних задач, простоти масштабування. В свою чергу сучасна елементна база, а саме широка різноманітність мікроконтролерів *MPU* (*Microprocessor Unit*) та програмовні логічні інтегральні схеми (ПЛІС), обґрунтовує певні проблеми, які виникають під час проектування таких систем.

У статті розглядаються особливості сучасної методології створення мікропроцесорних систем (МПС) для вирішення широких класів завдань обробки інформації, зокрема завдань керування, що обумовлені використанням сучасних *MPU* і ПЛІС.

2. Огляд сучасної елементної бази для створення мікропроцесорних систем

При проектуванні мікроконтролерів доводиться дотримуватися компроміс між розмірами і вартістю з одного боку і гнучкістю і продуктивністю з іншого. Для різних додатків оптимальне співвідношення цих та інших параметрів може значно відрізнятися . Тому існує величезна кількість типів мікроконтролерів, що відрізняються архітектурою процесорного модуля, розміром і типом вбудованої пам'яті, набором периферійних пристроїв, типом корпусу і т. д. На відміну від звичайних комп'ютерних мікропроцесорів, в мікроконтролерах часто використовується Гарвардська архітектура пам'яті, тобто роздільне зберігання даних і команд в ОЗУ і ПЗУ відповідно до рис 1.

Центральний процесорний пристрій	Постійний запам’ятовуючий пристій
Послідовний інтерфейс	Таймери

Рис. 1. Структурні компоненти мікроконтролера

Відмінність подібних систем від ПЛІС полягає у внутрішній структурі. Якщо логічна інтегральна схема складається з множини логічних схем та елементів, програмування представлене побудовою зв’язків між ними, то мікроконтролер формує сигнали виходячи з відповідних команд пам’яті програм. Сучасні мікропроцесорні системи дотримуються визначеної архітектури (рис. 2), вона досить легко простежується у керувальних пристроях відомих виробників (*Arduino, Seeeduino, Iskra*).

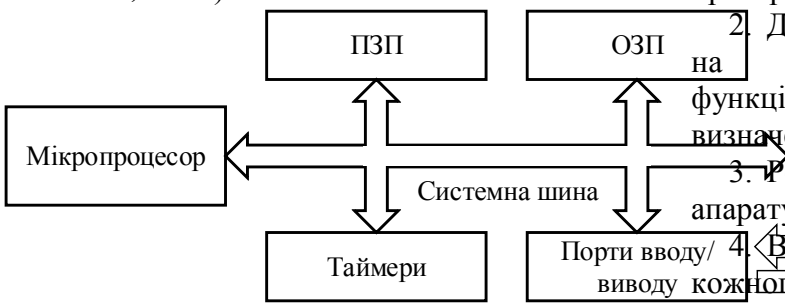

Рис. 2 . – Структура мікропроцесорної системи

Таке поєднання периферійних пристроїв є оптимальним, забезпечуючи користувача необхідними засобами для використання про цьому не обтяжуючи систему з метою підвищення швидкодії.

3. Особливості структурного синтезу сучасних мікропроцесорних систем

Основною проблемою з огляду функціональних можливостей є забезпечення сукупності критеріїв функціонування систем, які забезпечують оптимальне співвідношення проективності і витрачених ресурсів на створення системи обробки інформації. Такими критеріями є висока продуктивність, швидкодія, надійність, гнучкість архітектури, мінімізація розмірів та вартості [2]. Особливістю початкових етапів процесу проектування є аналіз, який дозволяє виявити суттєві ознаки функціонування об'єкта керування і підходи до оптимізації системи з метою отримання найкращих показників функціонування.

Наступним етапом є структурне проектування. Структурне проектування МПС полягає в реалізації регламентованої послідовності дій з проектування апаратних засобів і вибору структури програми, що дозволяють розробити системи керування, які відповідають заданим технічним вимогам. Структурне проектування МПС не завжди гарантує успішне завершення проекту, але значно збільшує його ймовірність.

Зазвичай використовують наступні етапи структурного проектування [3]:

1. Детальний аналіз вимог, що пред'являються до проектованого пристрою, на основі яких формуються технічні характеристики розроблюваного пристрою;
2. Декомпозиція проектованої системи на кілька взаємопов'язаних функціональних підсистем (модулів) з визначенням взаємозв'язків між ними.
3. Розробка структурної схеми апаратури та алгоритму її функціонування;
4. Визначення способу реалізації кожного функціонального модулю (вибір апаратних та програмних рішень);
5. Комплексне налагодження проектованого пристрою.

4. Інструментальні засоби розробки МПС

Особливістю створення і налагодження мікропроцесорних систем є те, що для програмування даної системи як правило, не достатньо одного лише мікроконтролера, це пов'язано з дефіцитом власних ресурсів системи. Для чого розробники мікроконтролерів пропонують спеціальні інструментальні засоби розробки і налагодження МПС [4].

За функціональним призначенням засоби розробки можна класифікувати наступним чином:

1. *Оціночні і демонстраційні плати*. Дозволяють в короткі терміни розробити пристрій.
2. *Схемні емулятори*. Налагоджувальні інструменти, що представляють собою набір апаратно-програмних засобів і дозволяють заміщати собою емульований мікроконтролер у реальній схемі.
3. *Програмні симулятори*. Програмні засоби для імітації роботи мікроконтролера.
4. *Налагоджувач*і. Дозволяють користувачеві контролювати хід виконання програми і бачити відповідність між вихідним текстом, образом програми в

машинних кодах та станом всіх ресурсів мікроконтролера.

5. *Емулятори ПЗП*. Програмно-апаратні засоби для завантаження програми за допомогою комп'ютера через один зі стандартних інтерфейсів.

6. *Програматори*. Пристрої, що дозволяють програмувати пам'ять мікроконтролера та програмовані логічні інтегральні схеми.

7. *Інтегровані середовища розробки*. Надають універсальний інтерфейс для роботи з усіма компонентами пакету.

Реальні засоби розробки МПС часто об'єднують в собі різні функції та режими роботи. Сучасні програмні засоби розробки дозволяють розробляти програми з використанням як низькорівневих (*Assemler*), так і високорівневих мов програмування (*C, C ++, Java*), що в комплексі з великою кількістю бібліотек дозволяє з мінімальними зусиллями досягти необхідного результату шляхом виконання елементарних задач.

5. Реалізація основних етапів проектування МПС

Як правило МПС це ієрархічна система, що обумовлює її функціональну й топологічну децентралізацію. Метою функціональної децентралізації системи контролю та управління є зниження складності системи шляхом розділення функцій системи на більш дрібні, тобто на підпроцеси. При цьому поділ функцій здійснюється так, щоб забезпечити задоволення вимог представлених критеріїв. Тому помилки, допущені на етапі формування критеріальною системи оцінок, не дозволяють провести адекватну децентралізацію системи.

У ряді випадків технічний процес легко розбивається на кілька слабов’язанних підпроцесів, кожен з яких може бути реалізований на окремому мікроконтролері, завдяки чому значно знижується складність кінцевої системи обробки інформації. Однак інші технічні процеси більш складні, і їх розбиття породжує сильно взаємопов'язані підпроцеси.

Звідси випливає один з підходів до синтезу системи обробки інформації, такий як оптимальна функціональна децентралізація системи управління або моніторингу, яка має на увазі розбиття цілісного процесу на такі підпроцеси, які слабо пов'язані між собою, тобто пов'язані між собою через мінімальний інтерфейс. При такому підході до проектування "зверху - вниз" здійснюється початкове розбиття цілісної системи на окремі модулі, після чого завдання синтезу окремих локальних систем на базі мікроконтролера не представляє великої складності. Такий підхід добре використовується при завданнях технічного моніторингу, коли цілісний технічний процес контролю параметрів дійсно досить легко розбивається на окремі підпроцеси. При синтезі системи обробки інформації не завжди вдається здійснити таке розбиття. Це породжує більш складні підходи до задачі формалізації проектування системи обробки інформації.

Одним з методів проектування складної системи управління є генерування усіх можливих варіантів побудови системи з метою вибору найкращого з них за кількістю максимально можливих значень критеріїв [3]. При традиційному підході до проектування з представлених законів управління в підсистемах необхідно було б необхідно виключити ті, які при дії на підсистему зовнішніх чинників не забезпечують потрапляння в задану область розкиду вихідних змінних при заданих початкових умов. З позиції багатоваріантного підходу це призводить до необґрунтованого звуження безлічі варіантів системи і тим самим не дозволяє сформувати найкращий варіант з вже розроблених систем управління окремими операціями.

Щоб не втратити жодного варіанту системи з кращими значеннями за іншими критеріями, залежить від законів управління в підсистемах, необхідно здійснювати оцінку системи в цілому з урахуванням повної сукупності можливих варіантів її створення.

Такий підхід має місце при автоматизованому проектуванні МПС. Однак його недоліки очевидні – це висока

абстрактність і складність математичного апарату дослідження, в наслідок яких часто зникає суть самої синтезованої системи управління. Часові та матеріальні витрати значно зростають, а оптимальним варіантом проектованої системи може виявитися той же самий, який міг бути отриманий при класичному системному підході до проектування.

Інший підхід до синтезу системи обробки інформації полягає в послідовному виконанні таких процедур, як розробка методів формального опису і дослідження функціонування системи і її модулів; створення узагальнених модулів функціонування комплексу технічних засобів; розробка математичних методів розрахунку параметрів комплексу; створення засобів автоматизації розрахунків; розробка методів синтезу складу і системи; розробка методів контролю результатів.

Особливий інтерес представляє методика синтезу МПС, заснована на ієрархічному підході з описом на певному рівні абстракції. Основою цієї методики проектування є процедура генерування структурних (*S*) і параметричних (*P*) моделей при заданої функціональної (*F*) моделі системи. Опис системи здійснюється за допомогою її функціональної, структурної та параметричної моделі <*F*, *S*, *P*>. На основі цих трьох моделей можна вирішувати задачу оптимального синтезу системи за деяким критерієм. Ця методика проектування передбачає системний підхід і інтегрує такі важливі принципи: ієрархічної багаторівневої системи; багаторівневого багатофункціонального моделювання, структурного програмування; систематизованих підходів до прийняття проектних рішень і перевірки їх коректності.

6. Висновки

У даній статті було досліджено методологію та основні етапи розробки системи обробки інформації на базі мікроконтролерів. Такий підхід до створення систем управління значно підвищує швидкодію пристроїв за рахунок розподілення задачі на елементарні процеси, що виконуються на мікроконтролерах циклічно без використання додаткових програмних та апаратних ресурсів

Досвід промислового використання мікрокопроцесорних систем управління показує, що для виявлення несправностей і подальшого відновлення працездатності широко використовуються методи сигнатурного моніторингу, що забезпечують відмовостійкість системи за допомогою програмно-апаратних засобів, вбудованих на кристал або друковану плату.

Список використаних джерел

1. Новиков Ю. В. Основы микропроцессорной техники. Учебное пособие / Ю. В. Новиков, П. К. Скоробогатов., 2009. – 336 с.

2. Онипенко А. П. МЕТОДЫ АНАЛИЗА И СИНТЕЗА РАСПРЕДЕЛЕННЫХ МИКРОКОНТРОЛЛЕРНЫХ СИСТЕМ УПРАВЛЕНИЯ СЛОЖНЫХ ИЕРАРХИЧЕСКИХ ОБЪЕКТОВ / А. П. Онипенко. // Известия Южного федерального университета. Технические науки. – 2001. – С. 44. 4 р

3. Шегал А. А. ПРИМЕНЕНИЕ ПРОГРАММНОГО КОМПЛЕКСА MULTISIM ДЛЯ ПРОЕКТИРОВАНИЯ УСТРОЙСТВ НА МИКРОКОНТРОЛЛЕРАХ / Анна Айзиковна Шегал. // Издательство Уральского университета. – 2014. – С. 8.

4. Гурин А. Программно-инструментальные средства разработки и отладки [Електронний ресурс] / А. Гурин, П. Перевозчиков // РадиоЛоцман. – 2004. – Режим доступу до ресурсу: http://www.rlocman.ru/review/article.html?di=1809.

УДК 004.93(015.7)

АНТОШКИН Р.О.,
КУЛАКОВ Ю.А.

КОНСТРУИРОВАНИЕ ТРАФИКА В ПРОГРАММНО КОНФИГУРИРУЕМЫХ СЕТЯХ.

В наше время сети активно развиваются и требуют постоянного усовершенствования. Среди множества решений стоит выделить программно-конфигурируемые сети (SDN), главная идея которой заключается в отделении функций передачи трафика от функций управления. Реализация концепции SDN на практике позволит предприятиям и операторам связи получить независимый контроль над всей сетью из единого места, что значительно упростит ее эксплуатацию. Эти и остальные преимущества SDN сетей будут рассмотрены в данной статье.

Nowadays networks are actively developing and require constant improvement. Among the many solutions is the Software Defined Networking (SDN), the main idea of which is to separate the functions of traffic transmission from control functions. The implementation of the SDN concept in practice will allow enterprises and telecom operators to get independent control over the entire network from a single location, which will greatly simplify its exploitation. These and the rest of advantages of SDN networks will be discussed in this article.

Ключевые слова: программно-конфигурируемые сети, управление трафиком.

1. Введение

Основной проблемой сети передачи данных является динамический характер сетевых приложений и их среды. Это означает, что требования к производительности передаваемых потоков данных, например, Quality of Service (QoS), могут меняться со временем. Приложения работают в широком диапазоне сред, т.е. проводных и беспроводных, с различными сетевыми устройствами. Для эффективной работы приложений базовая сеть должна быть достаточно гибкой, чтобы динамически меняться в ответ на любые изменения в требованиях приложения и их окружении. Существующие подходы основаны на статических, сверх зависимых оверлейных сетях, либо требуют изменения приложений в соответствии с производительностью сети.

Важным способом решения этой проблемы является разработка трафика (TE). Это процесс анализа состояния сети, прогнозирования и балансировки передаваемой нагрузки данных по сетевым ресурсам. Это метод, используемый для адаптации маршрутизации трафика к изменениям в состоянии сети. Однако эти методы не обеспечивают дополнительных ресурсов для трафика, который требует QoS. Традиционные методы маршрутизации не обеспечивают какой-либо механизм для распределения сетевых ресурсов оптимальным образом.

Компьютерные сети состоят из множества сетевых устройств, таких как коммутаторы, средние блоки (например, межсетевые экраны) и маршрутизаторы. Операторы сетей должны вручную настроить эти устройства для различных приложений, чтобы реагировать на различные приложения и события в сети. Часто им приходится использовать ограниченные инструменты, такие как интерфейс командной строки (CLI) и иногда инструменты для создания сценариев для преобразования этих политик конфигурации высокого уровня в политики низкого уровня. Это затрудняет управление и оптимизацию сети, что может привести к ошибкам в сети. Другие проблемы с этой архитектурой могут вызвать колебания в сети, поскольку плоскости управления устройств распределены, нововведение затруднено, поскольку поставщики запрещают модификацию базового программного обеспечения в устройствах. Чтобы преодолеть эти проблемы, была введена идея программирования сети Software Defined Networking (SDN).

2. Описание технологии Software Defined Networking (SDN)

Главная идея SDN заключается в отделении функций передачи трафика от функций управления (включая контроль, как самого трафика, так и осуществляющих его передачу устройств). В традиционных коммутаторах и маршрутизаторах эти процессы неотделимы друг от друга и реализованы в одной «коробке»: специальные микросхемы обеспечивают пересылку пакетов с одного порта на другой, а вышележащее ПО определяет правила такой пересылки, выполняет необходимый анализ пакетов, производит изменение содержащейся в них служебной информации и т д. (Рис. 1)**.** Для определения маршрута передачи или недопущения зацикливания трафика устройства, конечно, «общаются между собой», для чего разработано множество протоколов, таких как OSPF, BGP и Spanning Tree, но при этом каждое функционирует автономно.

отслеживать работу всей сети (Рис. 2). Согласно замыслу разработчиков, SDN позволит программировать сеть как единое целое, а администраторам не придется заниматься отдельными устройствами. Главным становится контроллер: он все видит, все знает и раздает сетевым устройствам инструкции по обработке трафика. Самим устройствам больше не надо разбираться в сотнях замысловатых протоколов — достаточно следовать инструкциям контроллера, а значит, они могут быть простыми и дешевыми.

Реализация концепции SDN на практике позволит предприятиям и операторам связи получить контроль над всей сетью из единого места, что значительно упростит ее эксплуатацию. Что не менее важно, конфигурирование сети сильно упростится и администраторам не придется вводить сотни строчек кода отдельно для разных коммутаторов или маршрутизаторов. Характеристики сети можно будет

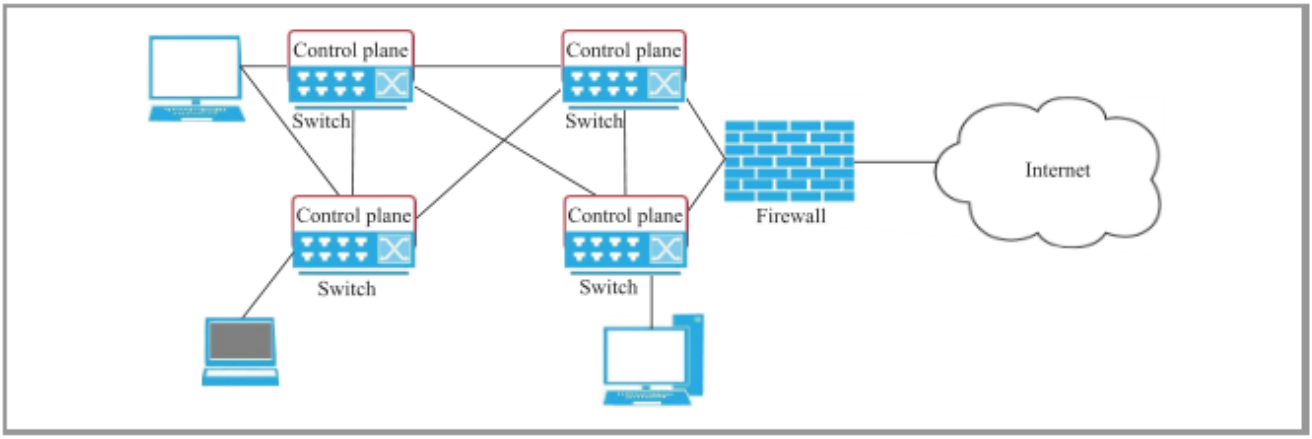

Рис. 1 Архитектура традиционной сети

Согласно концепции SDN, вся логика управления выносится в так называемые контроллеры, которые способны оперативно изменять в режиме реального времени, соответственно, сроки внедрения новых приложений и сервисов значительно

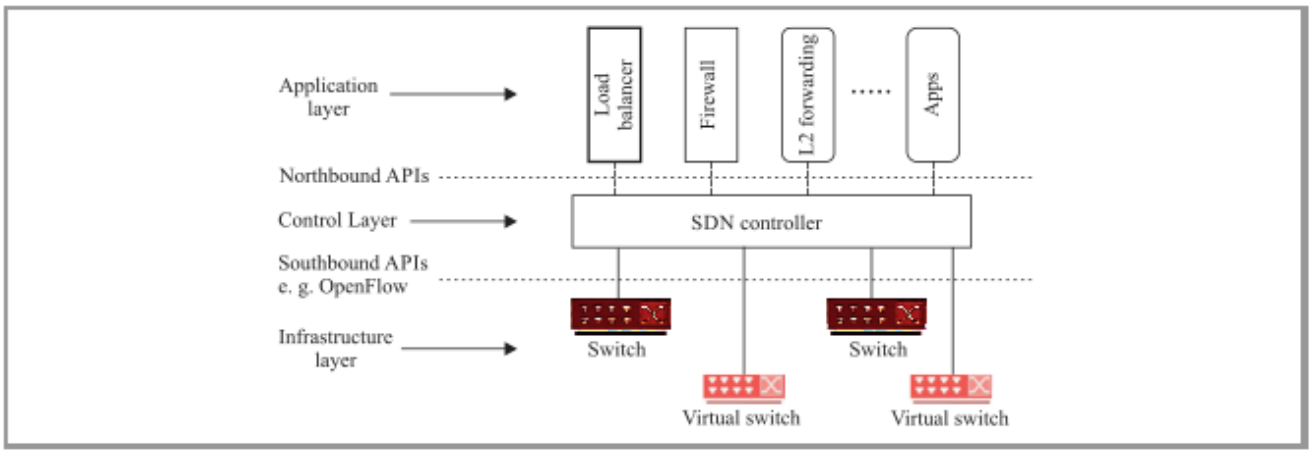

Рис.2 Архитектура SDN сети

сократятся.

Основным элементом концепции SDN является протокол OpenFlow, который обеспечивает взаимодействие контроллера с сетевыми устройствами (Рис. 2). На «северной» стороне контроллер предоставляет программные интерфейсы (API), наличие которых позволяет владельцу сети или сторонним разработчикам создавать приложения для управления сетью. Такие приложения могут выполнять самые разные функции в интересах бизнес-задач (например, контролировать доступ, управлять пропускной способностью и т. п.), причем их разработчикам не надо знать детали функционирования конкретных сетевых устройств. Благодаря контроллеру, вся сеть, состоящая из множества разнотипных устройств разных производителей, предстает для приложения как один логический коммутатор.

Преимущества, которые дает SDN, очевидны, причем не только для сетей в центрах обработки данных, но и для других типов сетевых инфраструктур. Централизованное управление средой, значительное упрощение обслуживания и модернизации, сокращение времени на обновление программных кодов коммутаторов/маршрутизаторов и внедрение новых сервисов — все перечисленное важно, как для корпоративных сетей, так и для инфраструктур операторов связи. Однако это не повод разом отказываться от преимуществ развиваемого десятилетиями традиционного подхода, когда каждое сетевое устройство наделяется «интеллектом», достаточным для автономного функционирования.

3. Обзор классических решенийконструирования трафика

Классические методы организации трафика основаны на тонкой настройке TE и механизма маршрутизации, таких как ECMP или существующие протоколы маршрутизации, такие как IS-IS или MPL. Протоколы маршрутизации Open Shortest Path First (OSPF) и IS-IS не адаптируются к изменениям в состоянии сети, поскольку вес ссылок является статическим, и при выборе путей эти протоколы не имеют цели достигнуть максимальной производительности. Расширения технической инфраструктуры IS-IS и стандарта OSPF расширяют эти протоколы за счет включения нагрузки трафика при выборе пути. В этих подходах во время объявления состоянии канала связи маршрутизаторы объявляют нагрузку на трафик вместе со стоимостью канала. После того, как маршрутизаторы обмениваются ссылками и трафиком, они вычисляют кратчайший маршрут для каждого пункта назначения. Эти стандарты требуют изменения маршрутизаторов для сбора и обмена статистикой трафика.

Multi-Protocol Label Switching, MPLS, обеспечивает механизм туннелирования. Он создает сквозные соединения между узлами. MPLS может интегрировать метки коротких путей с механизмом IP-маршрутизации, где входящие маршрутизаторы назначают коротким фиксированным меткам для пакетов вместо длинных сетевых адресов. Сетевые устройства используют этот ярлык для пересылки пакетов к месту назначения посредством маршрута с коммутацией меток (LSP). Это уменьшает издержки на поиск таблицы маршрутизации. На основе MPLS-TE, основанной на MPLS-технологии, сначала резервируются ресурсы для сквозного маршрута, а затем передаются данные. Он устанавливает маркированный коммутируемый путь по ссылкам с достаточной пропускной способностью. Этот метод обеспечивает достаточное количество ресурсов для потока. Поскольку MPLS-TE работает с доступной пропускной способностью в одном агрегированном классе, он не поддерживает QoS. Для обеспечения возможности QoS были внедрены технологии MPLS-TE, основанные на DiffServe, которые сочетают в себе технологии управления дифференцированными услугами (DiffServ) и MPLS для обеспечения QoS. По сравнению с обычным протоколом маршрутизации MPLS является более гибким в выборе путей, поскольку он настраивает пути виртуальных каналов для отправки трафика. Недостатком MPLS является то, что сетевые операторы должны управлять распределением ресурсов по каждому пути и изменять конфигурацию сети, чтобы

настроить путь согласно передаваемому трафику. Поскольку MPLS-TE передает агрегированый трафик по выделенным LSP, он страдает отсутствием гибкости. В MPLS-TE необходимо использовать резервные ссылки, чтобы в случае сбоя какой-либо ссылки трафик мог передаваться по различным путям.

Большинство обсуждаемых подходов согласуются с тем, что для эффективной разработки трафика необходим общесистемный подход. Когда в объеме трафика происходят кратковременные изменения, решение по управлению трафиком должно быстро решить, как распределить трафик по разным путям, чтобы использовать канал сбалансировано. В таких обстоятельствах, когда структура трафика изменяется часто, важно, чтобы решение по управлению трафиком было стабильным. В противном случае это может вызвать колебания. Колебания трафика могут иметь ряд нежелательных эффектов в сети, например, переполнение буфера коммутатора, нестандартные пакеты, плохое распределение сетевых ресурсов для пользователей, задержка трафика и ухудшение обслуживания. Решения, которые не имеют вышеуказанных недостатков, трудно реализовать в традиционной сетевой архитектуре, поскольку нам необходимо иметь доступ к глобальной информации в режиме реального времени, что является утомительной работой в этой парадигме. Чтобы найти оптимальное решение, большинство предлагаемых решений основаны на локальных измерениях, т.е. требуют, чтобы сетевые устройства самостоятельно определяли, как отправлять пакеты. Как правило, в традиционных сетях цена связи сохраняется статичной в течение длительного периода времени. Поскольку стоимость канала фиксирована, трафик передается по одному и тому же маршруту, пока не изменятся затраты на связь.

Для того, чтобы техника трафика имела оптимальный эффект в сети, она должна иметь следующие характеристики:

• она должна использовать многолучевое разнесение в сети,

• она должна принимать решения о маршрутизации на основе глобального состояния сети.

• она должна учитывать значения потока.

4. Конструирование трафика в программно конфигурируемых сетях

В сетях на базе SDN контроллер может динамически изменять состояние сети, например, в традиционных сетях стоимость канала для протоколов маршрутизации, таких как IS-IS, сохраняется в течение длительного времени. Если в сети происходит перегрузка, это может привести к плохой доставке данных, пока не изменятся затраты на связь или проблема не будет решена. Однако в SDN эти значения могут быть изменены более динамично, чтобы адаптироваться к изменениям. Можно реализовать более инновационный механизм маршрутизации или изменить существующие протоколы маршрутизации, чтобы они могли динамически меняться в зависимости от состояния сети, чтобы повысить эффективность использования ресурсов, избежать сбоев и перегрузок и улучшить качество обслуживания.

Протокол OpenFlow при идентификации трафика оперирует понятием «потока». Ключевым элементом коммутатора, поддерживающего этот протокол, является таблица потоков (Flow Table). Группа столбцов в левой части таблицы формирует поля соответствия, где указаны характеристики потоков: это могут быть различные параметры, включая MAC- и IP-адреса отправителя и получателя, идентификатор VLAN, номера протокольных портов TCP и UDP, а также другая информация. Эти данные с помощью протокола OpenFlow записывает в таблицу коммутатора контроллер, он же определяет приоритет разных потоков: чем выше приоритет, тем выше соответствующая запись в таблице потоков.Входящие пакеты проверяются на соответствие указанным в таблице параметрам. Если соответствие выявлено, к пакетам применяется действие, которое указано в следующем столбце таблицы. Типичным действием является пересылка пакета на один или несколько выходных портов. Кроме того, коммутатор может изменить содержимое служебных

полей пакета, сбросить его, направить для анализа контроллеру и т. д. В случае если совпадение не найдено, пакет сбрасывается или направляется контроллеру, который определит, как следует обрабатывать данный поток, и добавит соответствующую запись в таблицу. Статистика по проходящему трафику — число пакетов, байтов и пр. — помещается в соответствующие поля (на Рисунке 3 они обозначены как Count).

Используя протокол OpenFlow, контроллер добавляет, модифицирует и удаляет записи в таблице потоков. Кроме того, он может запрашивать у коммутатора его характеристики и собранную статистику, конфигурировать коммутатор и его отдельные порты.

Разделение «плоскостей» передачи и управления можно реализовать вообще не затрагивая имеющуюся физическую сеть — задействуя виртуальные коммутаторы наподобие Cisco Nexus 1000v, VMware DVS, IBM 5000v или даже Open vSwitch с открытым исходным кодом (см. Рисунок 4). Программирование таких коммутаторов с помощью контроллера позволяет создать виртуальную сеть SDN поверх имеющейся физической инфраструктуры. Некоторые эксперты рассматривают этот подход как альтернативу развиваемому ONF, но на самом деле, поскольку описываемая схема не исключает возможности использования стандартного протокола OpenFlow, противопоставлять ее решениям ONF не стоит.

Если в такой сети обычные коммутаторы также будут поддерживать OpenFlow, то к виртуальной сети можно будет подключить и физические серверы. Управление такими коммутаторами тоже можно будет передать контроллеру, если это не войдет в противоречие с принципом разделения физической и виртуальных сетей. Этот пример показывает, что в модели SDN конкретная реализация коммутатора — будь то физическое устройство или программа на гипервизоре — не имеет принципиального значения, главное, чтобы он мог получать и исполнять инструкции контроллера.

В рамках своей стратегичи SDN ряд производителей заявили об открытии функционала операционных систем своих устройств через API. До сих пор настройка сетевых устройств производилась преимущественно через командную строку или Webинтерфейс. Но эти инструменты ограничены той оболочкой программирования, которую предлагает производитель. При наличии API можно использовать более широкий набор инструментов программирования и создавать приложения не только для настройки сетевого устройства, но и для программирования сетевой среды в целом. По сути, этот подход является альтернативой SDN, при этом он обеспечивает доступ к более широкому набору функций сетевых устройств, что потенциально позволяет реализовать больше возможностей, чем заполнение таблицы потоков.

В частности, наличие доступа через API непосредственно к функционалу сетевых устройств позволяет системам типа VMware vCenter программировать сеть — например, задавать настройки VLAN в рамках общих задач по развертыванию и обслуживанию виртуальных машин. Для многих производителей коммутаторов интеграция с системой vCenter чрезвычайно важна, поскольку она упрощает и автоматизирует процедуры конфигурирования сетей для сред виртуализации VMware.

5. Заключение

Благодаря отделению плоскости управления от плоскости данных и помещении ее в сервер, называемый контроллером, становятся доступными более гибкие пути конструирования трафика. Преимущества, которые дает SDN, очевидны, причем не только для сетей в центрах обработки данных, но и для других типов сетевых инфраструктур. Однако это не повод разом отказываться от преимуществ развиваемого десятилетиями традиционного подхода, когда каждое сетевое устройство наделяется «интеллектом», достаточным для автономного функционирования. Однако в скором будущем ожидается переход к SDN архитектуре, хотя скорее всего он будет осуществляться постепенно и предельно осторожно.

Список литературы

1. Коломеец А.Е, Сурков Л.В. Программно-конфигурируемые сети на базе протокола OpenFlow // Электронный научно-технический журнал «Инженерный вестник» МГТУ им. Н.Э. Баумана. 2014. №5. 9 с. / URL:http://engbul.bmstu.ru/doc/711486.html
2. Коломеец А.Е, Сурков Л.В. Моделирование сетей SDN в среде Nicira // Электронный научно-технический журнал «Инженерный вестник» МГТУ им. Н.Э. Баумана».. 2014. №6. 6 с. / URL: http://engbul.bmstu.ru/doc/714126.html
3. Смелянский Р.Л. Программно-конфигурируемые сети // Открытые системы. 2012. №9. URL: http://www.osp.ru/os/2012/09/13032491/
4. OpenFlow Tutorial // OpenFlow.2013.URL: http://archive.openflow.org/wk/index.php/OpenFlow_Tutorial
5. ONF Specification // Open network foundation.2014. / URL: https://www.opennetworking.org/ja/sdn-resources-ja/onf-specifications
6. Thomas D. Nadeau, Ken Gray, SDN: Software Defined Networks, O'Reilly, 2013. pp 1025.
7. Черников А. С.1, Паус А. С. Многопоточная маршрутизации в программно-конфигурируемых сетях // Радиооптика. МГТУ им. Н.Э. Баумана. Электрон. журн. 2016. № 06. С. 35–46.
8. Mohammad R. Abbasi1, Ajay Guleria2, and Mandalika S. Devi Traffic Engineering in Software Defined Networks: A Survey // Department of Computer Science and Application, Panjab University, Chandigarh, India. Journal of telecommunications and information technologies