МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
Національний авіаційний університет
Навчально-науковий інститут
комп'ютерних інформаційних технологій

ЗБІРНИК
ТЕЗ ДОПОВІДЕЙ
X МІЖНАРОДНОЇ
НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«КОМП'ЮТЕРНІ СИСТЕМИ І МЕРЕЖНІ ТЕХНОЛОГІЇ»

(CSNT-2017)

20–22 квітня 2017 року

Київ 2017

УДК 004.7(043.2)

Збірник тез доповідей X Міжнародної науково-технічної конференції «Комп'ютерні системи і мережні технології» (CSNT-2017), м. Київ, 20–22 квітня 2017 р., Національний авіаційний університет. – К.: НАУ, 2017. – 96 с.

Рецензенти:

С. Д. Винничук – д.т.н., с.н.с., провідний науковий співробітник Інституту проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України;

В. Є. Мухін – д.т.н., доцент, професор кафедри обчислювальної техніки Національного технічного університету КПІ ім. І. Сікорського;

О. І. Стасюк – д.т.н., професор, проректор з наукової роботи Державного економіко-технологічного університету транспорту.

Збірник тез доповідей укладено за матеріалами X міжнародної науково-технічної конференції «Комп'ютерні системи і мережні технології» (CSNT-2017). У доповідях розглянуті наукові, технічні та технологічні проблеми побудови, проектування сучасних комп'ютерних систем, засоби і методи моделюваня комп'ютерних мереж, проблеми захисту ресурсів в інформаційних систмах, технології підготовки авіаційних фахівців.

Рекомендовано до друку вченою радою Навчально-наукового інституту комп'ютерних інформаційних технологій Національного авіаційного університету (протокол № 4 від 18 квітня 2017 р.).

ЗМІСТ

Андрєєв В.І., Андреєв О.В.
МЕТОД ТРИПАРАМЕТРИЧНОЇ ОПТИМАЛЬНОЇ ЕКСТРАПОЛЯЦІЇ ВИПАДКОВИХ НЕСТАЦІОНАРНИХ СИГНАЛІВ НА ТЛІ ЗАВАД, ЗАСНОВАНИЙ НА ВИКОРИСТАННІ ФУНКЦІЇ ЛАГРАНЖА…….7

Антонов В.К.
ЗАДАЧА О НЕСКОЛЬКИХ КОММИВОЯЖЕРАХ……9

Ахмедова Д.Н.
ОСОБЛИВОСТІ СТВОРЕННЯ РОБОТА-ГЕКСАПОДА…….11

Балакин С.В.
СРЕДСТВА ДИАГНОСТИРОВАНИЯ НЕСАНКЦИОНИРОВАННЫХ ВОЗДЕЙСТВИЙ И АТАК В КОМПЬЮТЕРНОЙ СЕТИ……...13

Боровик В.М., Рибасова Н.О.
МЕТОДОЛОГІЯ ПРОЕКТУВАННЯ БАЗ ДАНИХ ЗАСОБАМИ POWER DESIGNER……..15

Владимирський О.А., Мохор В.В., Плескач Б.Н., Кіндрась О.Л.
СИСТЕМА ДІАГНОСТУВАННЯ АЕС УКРАЇНИ……...17

Водопьянов С.В., Заруцкий В.А., Дрововозов В.И.
ПЕРСПЕКТИВЫ РАЗВИТИЯ КООПЕРАТИВНОГО ПОДХОДА В АЭРОНАВИГАЦИОННЫХ СИСТЕМАХ КРУПНЫХ АЭРОУЗЛОВ……19

Воробйов І.Є.
ТЕХНОЛОГІЯ FAST ETHERNET ТА ЇЇ ВІДМІННІСЬ ВІД ТЕХНОЛОГІЇ ETHERNET……..21

Галата Л.П., Пасічник П.В.
ЗАХИСТ КОМП`ЮТЕРНОЇ МЕРЕЖІ ЗА ДОПОМОГОЮ ПРОТОКОЛУ PPTP……..23

Гамаюн В.П.
РЕКОНФИГУРИРУЕМАЯ ОПЕРАЦИОННАЯ СТРУКТУРА……25

Гамаюн В.П., Комар А.А., Ильин И.Е., Липкин А.В.
ПРЕОБРАЗОВАТЕЛЬ КОДА В КВАЗИГРАФИЧЕСКИЙ ФОРМАТ……...27

Горіна В.В., Зудов О.М.
КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ РОБОТИ ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ В УМОВАХ ЗАВАД……29

Горіна В.В., Рибасова Н.О.
ОСОБЛИВОСТІ ПРОЕКТУВАННЯ ТА СТВОРЕННЯ ВЕБ-ЗАСТОСУВАННЯ……...31

Демчик В.В., Корочкін О.В., Русанова О.В.
ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ВИКОРИСТАННЯ ДРІБНОЗЕРНИСТОГО ПАРАЛЕЛІЗМУ В БАГАТОЯДЕРНИХ КОМП'ЮТЕРНИХ СИСТЕМАХ……33

Дрововозов В.І., Журавель Н.В.
ПІДВИЩЕННЯ НАДІЙНОСТІ ЗВ'ЯЗКУ В ЛОКАЛЬНИХ БЕЗДРОТОВИХ МЕРЕЖАХ……...35

Дубчак О.В., Мазур Я.С.
ПРОТОКОЛИ ТЕХНОЛОГІЇ VoIP……37

Жолдаков О.О., Жолдаков А.О.
АНАЛІЗ ПРОБЛЕМИ ФОРМУВАННЯ МІНІМАЛЬНОГО ПЕРЕЛІКУ ОБЛАДНАННЯ ПОВІТРЯНИХ СУДЕН, ЩО ЗАБЕЗПЕЧУЄ БЕЗПЕКУ ТА РЕГУЛЯРНІСТЬ ПОЛЬОТІВ……...39

Жуков І.А., Печурін М.К., Кондратова Л.П., Печурін С.М.
БАЛАНСУВАННЯ РОЗПОДІЛЕНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ПАРАЛЕЛЬНОЇ КЛАСИФІКАЦІЇ ОБ'ЄКТІВ……..41

Журиленко Б.Е.
МОДЕЛИРОВАНИЕ ПРОЦЕССА ВЗЛОМА И АНАЛИЗА РАБОЧЕГО СОСТОЯНИЯ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ……...43

Зюбіна Р.В., Бабенко Ю.М.
ОСОБЛИВОСТІ ІДЕНТИФІКАЦІЇ ЛЮДИНИ НА БАЗІ ГОЛОСОВОЇ БІОМЕТРІЇ……45

Кадет Н.П., Башкиров О.М.
ОЦІНКИ СТІЙКОСТІ ФУНКЦІОНУВАННЯ СИСТЕМИ ЗВ'ЯЗКУ В УМОВАХ НЕГАТИВНОГО ВПЛИВУ……..47

Капорін Р.М., Коган А.В.
СПОСОБИ ОРГАНІЗАЦІЇ БАГАТОШЛЯХОВОЇ МАРШРУТИЗАЦІЇ……...49

Кірхар Н.В., Ходаков Д.В.
ОСОБЛИВОСТІ ПРОГРАМУВАННЯ ПІД ANDROID……51

Ковалев Н.А.
ОРГАНИЗАЦИЯ ЛОГИЧЕСКИХ ВЫЧИСЛЕНИЙ……..53

Коган А.В., Храпов В.В.
МОДЕЛИРОВАНИЕ ТРАФИКА В MESH-СЕТЯХ С ОПРЕДЕЛЕННЫМ КАЧЕСТВОМ ОБСЛУЖИВАНИЯ……..55

Куц В.Ю., Іванов В.Г.
МЕТОД РЕЗЕРВУВАННЯ ТА ВІДНОВЛЕННЯ ДАНИХ В СИСТЕМАХ ЇХ ВІДДАЛЕНОГО ЗБЕРІГАННЯ……...57

Марковський О.П., Захаріудакіс Лефтеріос, Федотов М.Ф.
МЕТОД ШВИДКОЇ СТРОГОЇ ІДЕНТИФІКАЦІЇ ВІДДАЛЕНИХ КОРИСТУВАЧІВ…….59

Марковський О.П., Шапран К.О.
МЕТОД КОРЕКЦІЇ ОДНОКРАТНИХ ПОМИЛОК СИНХРОНІЗАЦІЇ В ПОСЛІДОВНИХ КАНАЛАХ ПЕРЕДАЧІ ДАНИХ…….61

Мелешко О.О., Коваль Д.Р.
ТЕХНОЛОГІЇ ПРИСКОРЕНОЇ РОЗРОБКИ FRONT-END……..63

Ничипоренко Л.О., Рудюк В.О.
СИСТЕМА ПРОДАЖУ ТА УПРАВЛІННЯ ТОВАРОМ……..65

Одарченко Р.С., Вергелес Д.Д., Абакумова А.О., Дика Н.В.
ВИЗНАЧЕННЯ ПЕРСПЕКТИВНИХ ВАРІАНТІВ ПОБУДОВИ ТРОПОСФЕРНИХ ЛІНІЙ ЗВ'ЯЗКУ……...67

Олещенко Л.М., Ландяк Д.П., Миколайчик В.В.
ОН-ЛАЙН СИСТЕМА ДИСПЕТЧЕРСЬКОГО УПРАВЛІННЯ АВТОБУСНИМИ ПАСАЖИРСЬКИМИ ПЕРЕВЕЗЕННЯМИ……..69

Опанасенко В.М., Эсанов Э.Э.
СТРУКТУРНАЯ ОРГАНИЗАЦИЯ УСТРОЙСТВ СОРТИРОВКИ НА БАЗЕ FPGA…….71

Пасічник П.В., Корнієнко Б.Я.
ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ FTP-СЕРВЕРА……73

Пащенко Н.В., Мокійчук В.М.
ІНФОРМАЦІЙНА СИСТЕМА УПРАВЛІННЯ ПРОЦЕСАМИ ЛАБОРАТОРІЇ……75

Petrenko S.O., Kudrenko S.O.
METHOD OF DETECTION MOVING OBJECTS
WITH DYNAMIC LIGHTING IN CCTV…….77

Пономаренко О.В., Булаковська Г.О.
ІЄРАРХІЧНА СИСТЕМА КОМП'ЮТЕРИЗОВАНОГО
УПРАВЛІННЯ ПРОДУКТОПРОВОДАМИ……..79

Ракицький В.А.
ПОРІВНЯЛЬНИЙ АНАЛІЗ WEB ТА LOTUS NOTES
НА РІВНІ СЕРВЕР – КЛІЄНТ…….81

Рудюк В.О., Ничипоренко Л.О.
СИСТЕМА ПРОЕКТУВАННЯ INTERNET ПРОВАЙДЕРА……...83

Rusanova O.V., Korochkin A.V.
SCHEDULING PROBLEMS FEATURES FOR
MODERN MULTICOMPUTER SYSTEMS……85

Толстікова О.В., Коцюр А.Б.
СИСТЕМА ОБРОБКИ ТА ВІДОБРАЖЕННЯ
АЕРОНАВІГАЦІЙНОЇ ІНФОРМАЦІЇ……...87

Феденко І.І.
АЛГОРИТМ ПІДВИЩЕННЯ ШВИДКОДІЇ АНАЛІЗУ
ТРАФІКУ В КОМП'ЮТЕРНИХ МЕРЕЖАХ……89

Чебаненко Т.М., Руденко Т.А.
ЗАХИЩЕНЕ МОДУЛЯРНЕ ЕКСПОНЕНЦІЮВАННЯ
У ХМАРНИХ СИСТЕМАХ…….91

Шмайденко М.С.
АНАЛІЗ ЗАСОБІВ HONEYPOT ЗА РІВНЯМИ ВЗАЄМОДІЇ
ЗІ ЗЛОВМИСНИКОМ……..93

УДК 519.218.82(043.2)

В. І. Андрєєв, к.т.н.,
О. В. Андреєв, к.т.н.,
Національний авіаційний університет, Київ

МЕТОД ТРИПАРАМЕТРИЧНОЇ ОПТИМАЛЬНОЇ ЕКСТРАПОЛЯЦІЇ ВИПАДКОВИХ НЕСТАЦІОНАРНИХ СИГНАЛІВ НА ТЛІ ЗАВАД, ЗАСНОВАНИЙ НА ВИКОРИСТАННІ ФУНКЦІЇ ЛАГРАНЖА

Вирішення задач екстраполяції випадкових процесів, до яких відноситься і трафік комп'ютерних мереж, займають важливе місце в різних галузях науки та техніки. Недостатньо вивченими залишаються задачі екстраполяції випадкових нестаціонарних сигналів (ВНС) на тлі стаціонарних та нестаціонарних завад.

Як подальший розвиток попередніх методів запропоновано метод оптимальної екстраполяції на базі функцій Лагранжа.

Ми маємо два спостереження ($n=2$), в результаті спостереження отримують значення Y_1 , Y_2 замість істинних значень X_1 , X_2 , по яким необхідно визначити за допомогою функції Лагранжа X_3, але насправді оптимально спрогнозувати значення Y^*_3.

Сигнал, що спостерігається, розглядається як «адитивна суміш» сигналу $Y(t)$ і завади $\xi(t)$:

$$Y(t) = X(t) + \xi(t) .$$

Задача екстраполяції полягає в тому, щоб у найкращий спосіб по значенням Y_1 , Y_2, що екстраполюються, отримати оцінку Y^*_3 майбутнього значення Y_3.

В основу методу поставлено задачу визначення оптимальних вагових коефіцієнтів α_{1opt} , α_{2opt} , а також невизначеного множника функції Лагранжа λ_{opt} за критерієм мінімуму дисперсії $minD_\varepsilon(\alpha_{1opt}$, α_{2opt} , $\lambda_{opt})$ похибки оптимального екстрапольованого значення випадкового нестаціонарного сигналу на тлі завад.

Для виконання екстраполяції необхідно мати набір апріорної ймовірностної інформаці про ВНС. Це наступний набір для точок спостереження Y_1, Y_2: математичті сподівання - m_{Y1}, m_{Y2}; дисперсії - D_{Y1}, D_{Y2} (або їх середньоквадратичні відхилення $\sigma_{Y1}{}^2$, $\sigma_{Y2}{}^2$); кореляційна функція - $K_Y(t_1, t_2)$. Крім того, треба визначити інтервали спостереження ΔT та екстраполяції τ , а також величину потужності завади σ^2_ξ Далі треба довизначити відсутніі параметри

для точки ВНС, яку збираємось екстраполювати: m_{Y3}, D_{Y3}, σ^2_{Y3}, $K_Y(t_1, t_3)$, $K_Y(t_2, t_3)$.

Оцінку Y_3^* істинного значення X_3 в момент часу t_3 розглядаємо як лінійну комбінацію (функцію) попередніх значень, що спостерігаються:

$$Y_3^* = \alpha_1 Y_1 + \alpha_2 Y_2 .$$

Вважаємо, що параметри α_1 , α_2 задовольняють вимозі нормування $\alpha_1 + \alpha_2 = 1$, тоді:

$$Y_3^* = Y_2 + \alpha (Y_1 - Y_2) .$$

Оцінка Y_3^* по формулі має наглядне пояснення: Y_2 – опорне значення, $\alpha(Y_1 - Y_2)$ – «добавка», яка є добутком $\Delta Y_{12} = Y_1 - Y_2$ значень сигналу на інтервалі спостереження та параметру екстраполяції α . Ставиться задача оптимізації оцінки значення $Y(t)$ в наступний момент часу t_{n+1} шляхом оптимального вибору параметру оптимізації α по відповідному критерію оптимізації.

Цільовою функцією оптимізації візьмемо функцію Лагранжа:

$$L(\vec{\alpha}, \lambda) = [A_0 + A_1 t_3^\gamma + \xi(t_3) - Y_3^*(\vec{\alpha})]^2 + \lambda[\sum_{k=1}^{2} \alpha_k - 1] ,$$

де $L(\vec{\alpha}, \lambda)$ – функція Лагранжа;

λ – невизначений множник Лагранжа;

$\vec{\alpha}$ – α_1, α_2 – вектор параметрів оптимізації;

$A_0 = \alpha_0$, $A_1 = \alpha_1$ являють собою випадкові незалежні величини, що мають гаусовські розподіли з математичними сподіваннями і дисперсіями, що визначені:

$$Y_3^*(\vec{\alpha}) = \alpha_1[A_0 + A_1 t_1^\gamma + \xi(t_1)] + \alpha_2[A_0 + A_1 t_2^\gamma + \xi(t_2)] =$$

$$= (\alpha_1 + \alpha_2) A_0 + (\alpha_1 t_1^\gamma + \alpha_2 t_2^\gamma) A_1 + \alpha_1 \xi(t_1) + \alpha_2 \xi(t_2) .$$

В роботі отримані формули за допомогою яких визначаються оптимальні параметри вище наведеного рівняння: оптимального екстрапольованого значення Y_3*, а також значення α_{1opt}, α_{2opt}, λ_{opt}, $D_\varepsilon(\alpha_1, \alpha_2, \lambda)_{min}$, $D[y_3^*]$. Відповідно до запропонованої методики було проведено моделювання в системі *MathCAD* методом статистичного імітаційного моделювання.Результати моделювання наглядно ілюструють новизну та ефективність методу, який має зручну для практичного використання форму.

УДК 004.073(043.2)

В. К. Антонов, д.т.н.
Национальный авиационный университет, Киев

ЗАДАЧА О НЕСКОЛЬКИХ КОММИВОЯЖЕРАХ

По аналогии с одной из самых известных задач комбинаторной оптимизации о коммивояжере, − которому требуется обойти заданное множество пунктов на карте по кратчайшему суммарному пути, поставим ту же задачу, увеличивая количество коммивояжеров. Это и составляет новизну предложения. Как и в традиционной постановке, у нас задача может быть замкнутой и не замкнутой, т.е. коммивояжерам может соответственно требоваться и не требоваться вернуться в исходный пункт.

Известны численные методы решения задачи об одном коммивояжере: метод сечений, метод ветвей и границ, различные простые эвристические численные процедуры. Известный механик и математик У. Гамильтон исследовал задачу о нахождении маршрутов на графе с 20 вершинами. Его работа считается одной из наиболее ранних в этом направлении.

В связи с очевидностью отсутствия аналитического компактного решения усилия математиков постепенно переместились на оценку объема вычислительной работы, что в итоге только обосновало отсутствие каких либо позитивных перспектив.

В нашем случае ситуация в этом плане, очевидно, становится существенно более безнадежной.

Тривиальное решение получается, когда их количество равно числу пунктов, и в каждом по одному коммивояжеру. Если их количество около половины числа пунктов, и они распределены достаточно равномерно, число вариантов решения не велико, поскольку требуется каждому в среднем один ход. При малых же количествах число вариантов решения увеличивается в сравнении с одним коммивояжером. Численные приемы решения задачи в этом случае не отличаются от традиционных, но приобретают некоторую иерархичность алгоритмов в силу зависимости оптимального плана от начального хода «несколькими фигурами».

В авиации приложение состоит в управлении несколькими беспилотными летательными аппаратами - коммивояжерами. Требуется обойти все заданные промежуточные пункты маршрута,

используя несколько беспилотников, в каждом пункте один из них должен быть не более одного раза, суммарный пройденный путь должен быть минимальным, и при этом каждый беспилотник имеет энергетическое ограничение ресурса пройденного пути.

В вычислительной технике возможна постановка решения множества задач ограниченным набором компьютеров. Задача подобна известной об оптимальном распределении вычислительных ресурсов (нескольких компьютеров) для решения наиболее быстро заданного набора вычислительных задач (возможно, с учетом приоритетности их решения).

Могут быть по аналогии предложены новые модификации известных игр, например игра в ГО при участии нескольких игроков по принципу один против всех.

Аналогия с задачами оптимальной самоорганизации тоже просматривается – ресурсы это коммивояжеры, а функции результирующей системы это пункты не подлежащие дублированию.

Наиболее интересна аналогия с принципами запрета в квантовой механике, где квантовая система как бы равномерно заполняется по квантовым числам – возможным степеням свободы – в полном соответствии с нашей задачей. При избытке «строительных блоков» образуется новая, в точности соответствующая исходной, частица материи, например атом. Его электронные энергетические уровни не содержат электронов с одинаковыми квантовыми состояниями. Множество электронов это коммивояжеры, а множество квантовых состояний это разные пункты маршрута. «Заготовка» для атома – пустой ящик с множеством разных похожих, но не повторяющихся ячеек. Но вот вопросы. – Откуда берутся эти ящики, почему они одинаковые? Их генерируют в геометрической прогрессии уже создавшиеся атомы? Здесь мы имеем дело, возможно, с некоторым новым принципом, включающим полноту заполнения квантовых уровней с условием максимальности разнообразия отдельных фрагментов частицы. Или так: «если рядом, то нечто максимально не похожее».

И главный - вопрос о том, не являются ли наши мысленные построения всего лишь ограниченной и не полной, но копией физической реальности?

УДК 004.896(043.2)

Д. Н. Ахмедова
НТУУ «КПІ ім. І. Сікорського», Київ

ОСОБЛИВОСТІ СТВОРЕННЯ РОБОТА-ГЕКСАПОДА

Сучасне покоління є свідком стрімкого розвитку науки та техніки. Одна з галузь, що розвивається – це робототехніка. Сьогодні роботи все більше впроваджуються в різні сфери людської діяльності, допомагаючи освоювати космос, удосконалювати медицину, розширювати можливості в різних областях науки, виробництво, військову техніку тощо. Робот - це автоматичний пристрій, що імітує рухи та/або дії людини. Існують різні види роботів і один з цих видів – це робот гексапод. Це платформа, яка використовує для пересування шість ніг.

Зазвичай в таких конструкціях присутні два або три сервоприводи на одній нозі, тобто в сумі 12 або 18 сервоприводів. Застосовуючи три сервоприводи можливо міняти положення в просторі як ніг, так і корпусу по всіх трьох осях, але такі рухи вимагають певних математичних розрахунків.

Для більш чіткої ходи використовується інверсна кінематика. Це тип планування руху, який використовується в основному в тих ситуаціях, коли необхідне точне позиціонування гнучких зчленувань одного об’єкта щодо інших об’єктів навколишнього середовища. Алгоритм інверсної кінематики забезпечує синхронне, коректне та правильне переміщення кінцівок робота.

Щодо операційної системи, то найкраща система для роботів – це ROS тому, що це дуже перспективний напрямок у робототехніці з безліччю інструментів і готових рішень для розробки. ROS (Robot Operating System) - це фреймворк для програмування роботів, що надає широкі можливості для розподіленої роботи. ROS забезпечує стандартні служби операційної системи, такі як: апаратну абстракцію, низькорівневий контроль пристроїв, реалізацію часто використовуваних функцій, передачу повідомлень між процесами і управління пакетами. ROS базується на архітектурі графів, де обробка даних відбувається в вузлах, які можуть отримувати і передавати повідомлення між собою. Бібліотека орієнтована на Unix-подібні системи. ROS має дві основні «сторони»: сторону операційної системи та набір підтримуваних користувачами

пакетів, які реалізують різні функції робототехніки: SLAM, планування, сприйняття, моделювання та інші.

Вище розглянута операційна система має бути встановлена на комп'ютер, наприклад, на одноплатний комп'ютер Raspberry PI, але керувати сервоприводами має спеціальний серво-контроллер. Цей контролер повинен мати 18 каналів для сервоприводів та інтерфейси USB та UART.

Робот-гексапод має високу прохідність і може перебувати в тих місцях, які не доступні людям: під завалами і в радіоактивних зонах. Досліджуючи територію, роботу необхідно передавати інформацію людям, які не мають можливості побачити, що коїться в недоступній зоні. Для цього роботу потрібна камера, яка буде передавати зображення на телефон або комп'ютер, що допоможе дізнатися чи є в небезпечній зоні люди або чи потрібна комусь допомога рятувальників.

Ця камера підключається до одноплатного комп'ютера Ruspberry Pi, а за передачу інформації відповідає операційна система ROS, яка приймає зображення з камери і транслює їх у мережу.

Важливе питання – це управління роботом, яке може буди виконано по Wi-Fi – з'єднанню, яке має ряд переваг:

1) Підвищений захист з'єднання;

2) Можливість використання різного діапазону частот (2,4 ГГц і 5 ГГц);

3) Дуже висока пропускна здатність в 600 мб / с (тоді як в Bluetooth з'єднанні всього 2 мб / с).

Створення гексапода - це дуже цікавий процес, а можливості ROS і продуктивність Raspberry Pi дозволяють додавати і вдосконалювати програмну складову робота.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. A Mathematical Introduction to Robotic Manipulation Richard M. Murray, Zexiang Li, S. Shankar Sastry. – 2012 , Maui, HI, USA. – p. 127-355.

2. RoboCraft. – Режим доступу.– http://robocraft.ru/.

3. Geoff Williams, CNC Robotics, Build Your Own Workshop Bot. - (Tab publisher, New York., 2009).

УДК 004.75(043.2)

С. В. Балакин, аспирант
Национальный авиационный университет, Киев

СРЕДСТВА ДИАГНОСТИРОВАНИЯ НЕСАНКЦИОНИРОВАННЫХ ВОЗДЕЙСТВИЙ И АТАК В КОМПЬЮТЕРНОЙ СЕТИ

Задача диагностирования несанкционированных воздействий и атак в компьютерной сети требует использования современных и эффективных методов способных корректно и своевременно ее выполнять. Процесс диагностирования должен реагировать на несанкционированные действия в сети и ориентироваться на их предотвращение. Средства диагностирования идентификации атак представляют собой новые технологии, которые имеют потенциал развития [1].

Предложена модель диагностирования несанкционированных воздействий и атак в компьютерной сети, а также разработана модель работы данной системы в режиме предотвращения и обнаружения опасной или подозрительной активности [2].

Сформированы требования к системам подлежащим к внедрению данных методов. Модуль диагностирования основан на методах отслеживания активности пользователя в сети, а при обнаружении несанкционированных действий или атак противодействовать им в режиме реального времени и своевременно реагировать на нарушения. Алгоритм диагностирования позволяет проводить обнаружение вторжений и предоставлять всю необходимую информацию для их анализа и предотвращения.

Предложена и рассмотрена реальная модель диагностирования атак, которая дает возможность обезопасить систему как от атак в самой системе, так и от внедрения в нее из сети.

Данная модель годится для разработки готового программного продукта для повышения достоверности идентификации вторжений. В перспективе присутствует возможность создания на основе метода бизнес-приложений для защиты информации в корпоративных системах и т.п. Выделены основные развивающиеся направления использования идентификации атак.

Решение задачи диагностирования заключается в инспектировании состояния системы на возникновение аномальной и несанкционированной активности. В методе используется сетка диагностирования (DN), позволяющая отслеживать действия пользователя и выявлять вторжения. Диагностирование системы происходит в режиме реального времени и позволяет своевременно реагировать на нарушения. В качестве характеристик для диагностирования берутся данные работы системы (S) на равных промежутках времени (t), а потом эти данные используются в DN для генерации отчетов про отличиях от эталонных значений в S и для формирования сообщений о несанкционированных действиях или подозрительной активности. При нормальной работе система продолжает функционировать в без изменений.

В работе также предложен метод учета времени активности пользователя, который отслеживает время рабочей сессии для того, чтобы выявлять возможный взлом системы (инсайдерские атаки).

В результате процесса диагностики анализируется и обрабатывается информация о деятельности защищенной системы. После диагностирования несанкционированных действий администратор сможет присекать те или иные несанкционированные обращения пользователя.

Информация о системе, за которой ведется наблюдение, поступает в виде отчетов. Безопасность системы и защита инфраструктуры могут быть встроены в систему диагностирования или быть отдельным элементом.

Концепция диагностирования воздействий и атак в компьютерных сетях открывает ряд вопросов изучения безопасности, и открывает перспективу расширения набора решаемых функциональных задач, а также является средством всестороннего усовершенствования сети.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Panos L. Effects-Based Feature Identification For Network Intrusion Detection − BrightLight Press, 2013. − 273 p.

2. Balakin S.V., Zhukov I.A. Detection of computer attacks using outliner method. −Young Scientist, 2016. − 91-93 pp.

УДК 004.94:004.422(043.2)

В. М. Боровик, к.т.н.,
Н. О. Рибасова, асистент
Національний авіаційний університет, Київ

МЕТОДОЛОГІЯ ПРОЕКТУВАННЯ БАЗ ДАНИХ ЗАСОБАМИ POWER DESIGNER

У роботі розглядається сучасний підхід у розробці моделей баз даних засобами Power Designer(PD). З моменту появи PD він розглядався як єдиний інструмент. Першочергово PD був розроблений для проектування моделей даних, но з часом ситуація змінилася і на даний момент у PD є 10 типів моделей для рішення різних задач моделювання та проектування.

Присутність більшого спектра моделей в одному інструменті дозволило досягти високого рівня інтеграції, який вряд чи був досягнутий у будь якому іншому випадку. PD представляє унікальне середовище, я якому можна одночасно працювати з моделями всіх типів у єдиному користувацькому інтерфейсі.

Оскільки ми маємо справу з загальним інтерфейсом, існує ряд функцій, доступних до усіх моделей, та набір функцій, індивідуальних для моделей конкретного типу.

До загальних функцій можна віднести:

– легко керовані вікна, які дозволяють відображати різні представлення ваших моделей;
– можливість налаштованих звітів;
– функції перевірки моделей;
– можливість генерувати код додатку та скрипти для баз даних;
– можливість зворотного проектування (RE), яка підтримується, наприклад, для фізичної(PDM) та об’єкто-орієнтованої моделі даних(OOM);
– палетта інструментів для кожного типу моделей.

Типи моделей:

– модель вимог;
– модель для побудови бізнес-процесів;
– концептуальна модель даних (CDM);
– логічна модель даних(LDM);
– фізична модель даних(PDM);

- модель переміщення даних;
- об’єктно-орієнтована модель(OOM);
- модель для побудови архітектури підприємства;
- вільна модель;
- проектування XML-схем.

Розробка будь-якої моделі починається через діалог New Model. Можливість внутрішньої синхронізації даних між моделями дозволяє організувати роботу з великою кількістю моделей PD. Взаємозв’язок та синхронізація між моделями визначається набором правил, залежних від типів зв’язаних моделей.

PD здатний синхронізувати моделі з файлами зовнішніх форматів, які можуть бути результатом розробки коду у середовищі програмування, скриптом для розробки чи зміни бази даних та ін.

Середовище моделювання PD дозволяє розробляти та використовувати складні комплексні взаємозв’язки між моделями.

Особливу увагу в PD приділяється зворотному проектуванню – процесу генерації PDM із існуючої схеми БД. Зворотне проектування(RE) виконується як у нову, так і в існуючу PDM.

Існують два способи виконувати зворотне проектування із розглядаємих схем баз даних:

- скрипт для генерації бази даних та інші скприпти;
- зворотне проектування виконується із існуючої БД, для чого задається джерело даних та параметри їх об’єднання.

Найбільш цікавим моментом є побудова моделі переміщення даних, яка дозволяє переміщувати інформацію із різних таблиць БД. Набори із різних таблиць бази повинні бути змінені різними способами (проекція, сортування, пошук, злиття, об’єднання, розділення та порівняння). Кожний з цих етапів має свої параметри та порядок. У ході моделювання переміщення даних описуються джерела даних, а також процеси їх загрузки та трансформації, які включають відповідні операції.

В останній частині технології розглядаються підготовчі етапи процесу розробки сховища даних. Нове сховище основане на існуючій концептуальній моделі.

На даний момент інтегровані системи проектування, подібні розглядаємій, складають гідну конкуренцію системам програмування, що робить їх реальним інструментом розробки додатків, інформаційних систем та бізнес-процесів.

УДК 681

О. А. Владимирський, к.т.н,
В. В. Мохор, д.т.н,
Б. Н. Плескач,
О. Л. Кіндрась
ІПМЕ ім. Г.Є. Пухова НАН України

СИСТЕМА ДІАГНОСТУВАННЯ АЕС УКРАЇНИ

Найважливіша роль атомної енергетики для України не викликає сумнівів. Проблема полягає в тому, що завершуються регламентні строки експлуатації більшості енергоблоків. Продовження термінів експлуатації можливе тільки при суттєвому підвищенні рівня прогнозування стану устаткування та конструкцій, що перебувають в особливо складних умовах експлуатації.

Розроблено проект концепції побудови багаторівневої галузевої системи моніторингу, діагностування і прогнозування технічного стану АЕС України (СМТС). Запропоновано при впровадженні СМТС застосовувати підхід «Плануй – Виконуй – Перевіряй – Дій» («plen-du-chek-act»). При цьому об'єктом управління є надійність основного енергетичного обладнання енергоблоку АЕС, суб'єктом управління є технічний, інженерний, керуючий персонал. Циклічний та поетапний підхід до впровадження СМТС дозволить прискорити її впровадження в практику та підвищити достовірність моніторингу. Розглянуто основні передумови та мета створення СМТС. Визначена стратегія технічного обслуговування обладнання. Розроблена структурна схема СМТС, передбачена можливість багаторазового горизонтального масштабування і нарощування функціональних можливостей впродовж розробки і впровадження нових алгоритмів діагностування та прогнозу. Розглянутий підхід, що набув назву Big Data Technology & Big Data Analysis. Обгрунтовано заходи щодо захисту інформації.

Структурна схема СМТС.

На рівні енергоблоків АЕС в даний час в процесі виконання програми з підвищення безпеки АЕС України проводиться впровадження дворівневих комплексних систем діагностики (КСД). Ці системи об'єднують кілька локальних систем діагностування (ЛСД) нижнього рівня, що здійснюють моніторинг і

діагностування основного обладнання реакторної установки. У перспективі передбачається охопити діагностуванням основне обладнання другого контуру, турбінне відділення та ін.

На рівні АЕС створюється захищена локальна діагностична мережа (ЛДМ), до якої підключаються КСД всіх блоків АЕС. В підрозділах, які займаються аналізом і використанням діагностичної інформації (управління ресурсом, ремонт, постачання та ін.), встановлюються робочі станції, підключені до ЛДМ.

На верхньому рівні створюється Центр діагностики (ЦД), який отримує діагностичну інформацію з АЕС по захищених каналах зв'язку. Формування інфраструктури підтримки технологій BigData доцільно на основі приватних хмар. Тут повинні бути зосереджені всі необхідні ресурси (обчислювальні, бази даних та ін.) для створення необхідних передумов успішної роботи експертів.

Основне завдання ЦД – управління створенням і впровадженням методичного, алгоритмічного, програмного (ПЗ) та апаратурного забезпечення для всіх рівнів СМТС, вибір пріоритетів і черговості вирішення завдань з урахуванням виробничої необхідності, економічної доцільності, наявного вітчизняного і міжнародного науково-технічного доробку, забезпечення єдиної технічної політики.

В якості ілюстрації можна привести проект підвищення показників достовірності підсистеми акустичного контролю протікання теплоносія першого контуру (СКПТ ПАК). В ІПМЕ ім. Г.Є.Пухова НАН України є позитивний досвід по розробці кореляційних методів реєстрації акустичних сигналів витоків протяжних ділянок підземних трубопроводів міських систем теплопостачання. Аналіз багаторічних архівів СКПТ ПАК дозволяє провести адаптацію наявних напрацювань для вирішення задачі підвищення чутливості і перешкодозахищеності системи. У разі успішного проходження етапу дослідної експлуатації на КСД одного з енергоблоків розглядається питання про доцільність встановлення нового ПЗ на інші енергоблоки.

Розробка та впровадження системи СМТС з використанням основних положень цієї концепції дозволить істотно покращити якість експлуатації обладнання та вийти на рівень обслуговування за фактичним технічним станом.

УДК 629.735.051:004.7 (043.3)

С. В. Водопьянов,
В. А. Заруцкий,
В. И. Дрововозов, к.т.н.
Національний авіаційний університет, м. Київ

ПЕРСПЕКТИВЫ РАЗВИТИЯ КООПЕРАТИВНОГО ПОДХОДА В АЭРОНАВИГАЦИОННЫХ СИСТЕМАХ КРУПНЫХ АЭРОУЗЛОВ

По результатам прогноза зарубежных экспертов [1,2], в 2025 году ситуация в сфере организации воздушного движения в Европе (при сравнении с современным состоянием) может выглядеть следующим образом: ожидаемое до 3-х раз увеличение интенсивности полетов в воздушном пространстве Европы; десятикратное улучшение фактора безопасности полетов; уменьшение стоимости операций по управлению воздушным движением (УВД) не менее чем в два раза; расширение номенклатуры сервисов; управление воздушным движением будет полностью базироваться на обмене данными; расширение полосы частот для задач полетов по маршрутам и для вспомогательных задач; новые радиосистемы; эволюция комплексной сетевой архитектуры в направлении сервис-ориентированной архитектуры (SOA); насыщение каналов связи вследствие роста интенсивности воздушного движения.

Как правило, показатели безопасности выражаются в виде частоты наступления какого-либо события, причиняющего вред.

Пример: интенсивность авиационных событий $\lambda = 10^{-6}$ (в среднем одно событие на 1 000 000 ч полета). Тогда при $t = 1000000 \div$ полета вероятность наступления авиационного события будет примерно $9{,}99899966 \times 10^{-1}$, т.е. почти единица.

Пусть теперь интенсивность авиационных событий $\lambda = 10^{-7}$ (фактор безопасности полетов в 10 раз выше).

Тогда при $t = 1000000 \div$ полета вероятность наступления авиационного события будет примерно $6{,}01879279 \times 10^{-1}$. Отметим, что при $t = 2000000 \div$ полета и $\lambda = 10^{-7}$ вероятность наступления авиационного события будет примерно $8{,}41499891 \times 10^{-1}$.

Графики вероятности наступления авиационного события при разных интенсивностях авиационных событий в зависимости от общего времени полетов приведены на рис. 1.

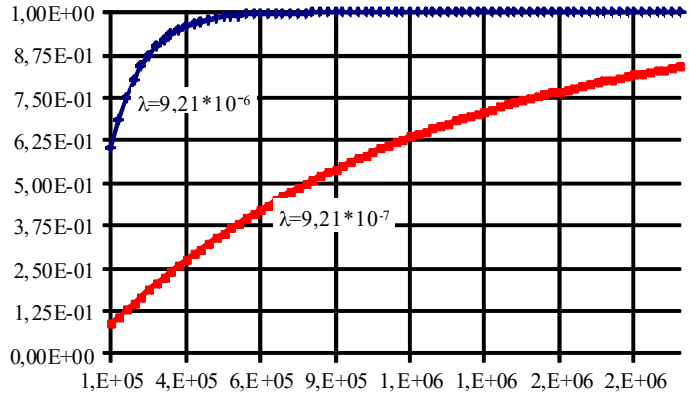

Рис. 1. Графики зависимости вероятности наступления авиационного события

Из анализа графиков (рис.1) можно сделать вывод, что при повышении фактора безопасности в 10 раз вероятность наступления авиационного события за 1 млн. часов полетов снижается с $9{,}99899966\times10^{-1}$ до $6{,}01879279\times10^{-1}$. Соответственно, вероятность полета в штатном режиме в конце интервала 1 млн. часов растет от $\approx 10^{-4}$ до $\approx 0{,}4$.

Другими словами, десятикратное повышение фактора безопасности полетов приводит к увеличению вероятности успешного полета примерно на 0,5.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Future Aeronautical Communications / Edited by Simon Plass. − Institute of Communications and Navigation, German Aerospace Center (DLR), Germany. – Published by InTech Janeza Trdine 9, 51000 Rijeka, Croatia. – InTech, 2011. – 378 p.

2. Aeronautical Air-Ground Data Link Communications / Mohamed Slim Ben Mahmoud, Christophe Guerber, Nicolas Larrieu, Alain Pirovano, José Radzik ISTE Ltd 27-37 St George's Road London SW19 4EU UK; John Wiley & Sons, Inc. 111 River Street Hoboken, NJ 07030 USA, 2014. − 127 p.

УДК 004.7:681.324

І. Є. Воробйов
Національний авіаційний університет, м. Київ

ТЕХНОЛОГІЯ FAST ETHERNET ТА ЇЇ ВІДМІННІСЬ ВІД ТЕХНОЛОГІЇ ETHERNET

Всі відмінності технології Fast Ethernet від Ethernet зосереджені на фізичному рівні (рис. 1). Рівні MAC і LLC в Fast Ethernet залишилися абсолютно тими ж, і їх описують колишні розділи стандартів 802.3 і 802.2. Тому розглядаючи технологію Fast Ethernet слід зупинитися тільки на декількох варіантах її фізичного рівня.

Складніша структура фізичного рівня технології Fast Ethernet викликана тим, що в ній використовуються три варіанти кабельних систем: волоконно-оптичний багатомодовий кабель, використовуються два волокна; вита пара категорії 5, використовуються дві пари; вита пара категорії 3, використовуються чотири пари.

Коаксіальний кабель, що відкрив світу мережу Ethernet, не потрапив в число дозволених середовищ передачі даних новій технології Fast. На великих відстанях оптичне волокно володіє набагато ширшою смугою пропускання, чим коаксиал, а вартість мережі виходить не високою.

Відмова від коаксіального кабелю привела до того, що мережі Fast Ethernet завжди мають ієрархічну деревовидну структуру, побудовану на концентраторах. Основною відмінністю конфігурацій мереж Fast Ethernet є скорочення діаметру мережі приблизно до 200 м.

В порівнянні з варіантами фізичної реалізації Ethernet (а їх налічується шість), в Fast Ethernet відмінності кожного варіанту від інших глибші - міняється як кількість провідників, так і методи кодування. А оскільки фізичні варіанти Fast Ethernet створювалися одночасно, а не еволюційно, як для мереж Ethernet, то була можливість детально визначити ті підрівні фізичного рівня, які не змінюються від варіанту до варіанту, і ті підрівні, які специфічні для кожного варіанту фізичного середовища.

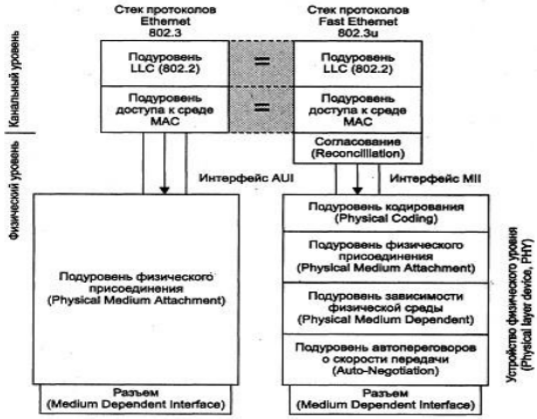

Рис. 1. Відмінності технології Fast Ethernet від технології Ethernet

Офіційний стандарт 802.3 встановив три різні специфікації для фізичного рівня Fast Ethernet і дав їм наступні назви: 100Base-TX для двохпарного кабелю на неекранованій витій парі UTP категорії 5 або екранованій витій парі STP Type 1; 100Base-T4 для чотирипарного кабелю на неекранованій витій парі UTP категорії 3, 4 або 5; 100Base-FX для багатомодового оптоволоконного кабелю, використовуються два волокна.

Для всіх трьох стандартів справедливі наступні твердження і характеристики.

- формати кадрів технології Fast Ethernet не відрізняються від форматів кадрів технологій 10-мегабитного Ethernet;

- міжкадровий інтервал (IPG) рівний 0,96 мкс, а бітовий інтервал рівний 10 нс. Всі тимчасові параметри алгоритму доступу (інтервал відстрочення, час передачі кадру мінімальної довжини і т. п.), зміряні в бітових інтервалах, залишилися колишніми, тому зміни в розділи стандарту, що стосуються рівня MAC, не вносилися;

- ознакою вільного стану середовища є передача по ній символу Idle відповідної надмірної коди (а не відсутність сигналів, як в стандартах Ethernet 10 Мбіт/с).

УДК 004.056.53

Л. П. Галата,
П. В. Пасічник
Національний авіаційний університет, Київ

ЗАХИСТ КОМП'ЮТЕРНОЇ МЕРЕЖІ ЗА ДОПОМОГОЮ ПРОТОКОЛУ PPTP

Основною особливістю будь-якої мережевої системи є те, що її компоненти розподілені в просторі і зв'язок між ними здійснюється фізично за допомогою мережевих з'єднань і програмно за допомогою механізму повідомлень. Мережеві системи характерні тим, що, поряд зі локальними атаками, до них застосуємо специфічний вид атак, так звані мережеві (або віддалені) атаки. Вони характерні , по-перше, тим, що зловмисник може знаходитися за тисячі кілометрів від об'єкта атаки, і, по-друге, тим, що нападу може піддаватися не конкретний комп'ютер, а інформація, що передається по мережі. З розвитком локальних і глобальних мереж саме віддалені атаки стають лідером, як по кількості спроб, так і по успішності їх застосування і, відповідно, забезпечення безпеки з точки зору протистояння віддаленим атакам набуває першорядного значення.

Протокол PPTP (Point-to-Point Tunneling Protocol) — тунельний протокол типу "точка - точка" дозволяє комп'ютеру встановлювати захищене з'єднання з сервером шляхом створення спеціального тунелю в стандартній незахищеній мережі.

Переваги протоколу PPTP:

- Використання приватного IP-адреси. Простір IP-адрес приватної мережі не повинен координуватися з простором глобальних (зовнішніх) адрес.
- Підтримка безлічі протоколів. Можна здійснювати доступ до приватних мереж, що використовують різні комбінації TCP / IP або IPX.
- Безпека передачі даних. Для запобігання несанкціонованого підключення використовуються протоколи і політики забезпечення безпеки сервера віддаленого доступу.
- Можливість використання аутентифікації і захисту даних при передачі пакетів через Інтернет.

В ОС сімейства Windows є можливість використання цього

протоколу. Для його налаштування з віддаленого клієнта необхідно налаштувати підключення в меню «Центр керування мережами і загальним доступом»> «Налаштування нового підключення або мережі»> «Підключення до робочого місця», відзначити галочкою пункт «Ні», створити нове підключення і далі вибрати «Використовувати моє підключення до Інтернету (VPN)».

В налаштуваннях підключення потрібно вказати зовнішній "білий" IP-адреса інтернет-центру (при підключенні з Інтернету) або локальний IP-адреса інтернет-центру (при підключенні з локальної мережі). Після цього необхідно вказати параметри облікового запису для підключення до PPTP-сервера:

Щоб трафік від PPTP-клієнта в віддалену підмережа за PPTP-сервером маршрутувався в VPN-тунель, а інший трафік прямував в основне звичайне підключення до інтернету, потрібно в настройках PPTP-підключення обов'язково прибрати галочку в полі «Використовувати основний шлюз в локальній мережі». При цьому маршрут в віддалену мережу за PPTP-сервером прийде автоматично, і мережу за VPN-сервером буде доступна без необхідності ручного додавання статичного маршруту.

Таким чином налаштувати та використовувати захищене з'єднання і бути впевненим в тому, що дані дійшли до адресату і не були перехоплені може простий користувач.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. В.Г. Олифер, Н.А. Олифер. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. − СПб.: Питер, 2010.−944с.: ил.
2. Корнієнко Б.Я. Система інформаційної безпеки / Д.П. Галата, Б.Я. Корнієнко, Л.П. Галата // Збірник наукових праць Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова. – 2011. – Вип. 59. − С. 48 - 52.
3. Корнієнко Б.Я. Прикладні програми управління інформаційними ризиками / Б.Я. Корнієнко, Н.М. Марутовська, Ю.О. Максімов / Захист інформації. – 2012, № 4 (57). − С. 60 - 64.
4. Корнієнко Б.Я. Оцінка ризиків автоматизованої інформаційної системи / Б.Я. Корнієнко, О.К. Юдін, Г.В. Наконечна // Наукоємні технології. – 2012. - № 2 (14). − С. 69-73.

УДК 004.(043.2)

В. П. Гамаюн, д.т.н.
Национальный авиационный университет, Киев

РЕКОНФИГУРИРУЕМАЯ ОПЕРАЦИОННАЯ СТРУКТУРА

Реконфигурация как направление в организации вычислительных структур широко применяется в исследованиях и разработке современных ЭВМ и систем.

Практически каждая часть операционной структуры разрабатывается с возможностью варьирования для преобразования в адаптивную, более производительную организацию. В целом реконфигурация предопределяет специализацию в соответствии с различным уровнем организации вычислительного процесса, процесса обработки. Специализация как форма организации для сокращения непроизводительных затрат применима к всем стадиям и слотам вычислительного процесса. Известны исследования системного характера, при которых программа-задание и архитектурно-структурное представление рассматриваются на системном уровне как объекты взаимной реконфигурации: программа и структура варьируются для уменьшения временных затрат при выполнении задания.

Некоторые другие аспекты- варианты предусматривают отдельную реконфигурацию программы и отдельную реконфигурацию структуры реализации. Подключение ряда функциональных узлов для увеличения производительности конвейера, применение линейки специализированных блоков, изменение системы коммутации и многое другое являются примерами реконфигурации. Либо объектом реконфигурации – специализации может быть структура, ориентированная на величину диапазона обрабатываемых данных.

Для достижения цели разработана система счисления, оптимизирующая выбор диапазона по критерию минимизации реализации операций - уменьшению количества шагов алгоритма как необходимых действий по преобразованию значащих разрядов. Такая система названа системой с плавающим диапазоном, адаптивной системы счисления (АСС).

В основе применяется принцип систем счисления в остатках. Главное отличие - использование изменяемой системы модулей для

представления чисел. Варианты применения того или иного модуля определяется «близостью» значения модуля и операнда.

Выбор модулей следующий – значение модуля равно уплотненному двоичному коду, что соответствует $m_1=15=1111_2$ $m_2=31=11111_2$ $m_3=63=111111_2$ …… $m_k = 2^k - 1=111…..1111$. Любое число (операнд), представленное в такой системе счисления, имеет следующий формат R/ H: первое поле R-ранг числа по модулю m_k, второе поле H - остаток числа по модулю m_k. Например, число 21 по модулю 15 определяется как - 1/6. Очевидно, что второе поле не превышает значения модуля, в первом поле может быть записано любое число.

Оптимизация при использовании адаптивной системы счисления заключается в минимизации значений представления операнда в двухполевом формате, так как эти значения являются объектами преобразования при выполнении арифметических операций.

Умножение чисел 21 и 17 с применением адаптивной системы счисления реализуется как:

$R_1*R_2*m + R_1*H_2 + R_2*H_1 = R_P$ - значение первого поля произведения;

$H_1*H_2= H_P$ - значение второго поля произведения.

Для выбранных чисел 21 и 17 получаем значение произведения 23/12.

При выборе модуля $31=11111_2$ полученное число 21*17 (1/6)*(1/2) представимо как 11/16, а при выборе модуля 63 как 5/42.

Оптимизация заключается в таком подборе значений двухполевой структуры представления операнда, которые обеспечили меньший диапазон действий при дальнейшей обработке. Например при модуле 15 имеем представление 23/12 , что уступает диапазону при модуле 31 – число представимо как 11/16. Преобразование операнда с одним модулем представления в представление с другим модулем реализуется за конечное количество операция сдвига и вычитания. Выбор оптимального представления – по величине диапазона операндов – предопределяет разрядность и, соответственно, структуру процессора.

УДК 004.(043.2)

В. П. Гамаюн, д.т.н.,
А. А. Комар,
И. Е. Ильин,
А. В. Липкин
Национальный авиационный университет, Киев

ПРЕОБРАЗОВАТЕЛЬ КОДА В КВАЗИГРАФИЧЕСКИЙ ФОРМАТ

Для выполнения макрооператорной, многооперандной обработки важное значение определяют количество значащих разрядов в разрядных сетках данных, так как являются фактором временных затрат на реализацию операции/команды. Предлагается способ представления операнда двумя объектами вместо разрядной сетки для числовых данных. Один объект соответствует позиции младшего разряда, другой объект (также кодовая комбинация) соответствует позиции старшего значащего разряда числового операнда. Принцип организации подобен применению кода «минус единица -1»: уплотненный двоичный код заменяется двумя кодами – код «-1» на позиции младшего разряда и 1 на позиции старшего разряда, увеличенного на +1: 1111111111
«код -1» = 1000000000(-1).

Недостатком является необходимость хранить все разряды двоичного операнда. Более перспективным является сочетание кода «-1» с разрядно-логарифмическим представлением (кодированием), при котором значащая единица кодируется номером позиции, в которой находится $N_i=\log_2 ap^i$. Поэтому рассмотренный код можно преобразовать к виду 1000000000(-1)= (11)(0) - где код (11) означает начало кода « -1», а (0) - окончание кода «-1».

Код «-1» применим к уплотнённым двоичным кодам, что уменьшает варианты его применения, другими словами нельзя применять этот код к любым двоичным кодам. Предложено использовать квазиграфический метод преобразования двоичных кодов, согласно которому многорядный двоичный код представим заполненной (единицами) матрицей уплотненных кодов. Выравнивание значений в разрядных срезах можно реализовать по следующему алгоритму: каждое число, равное значению

количества единиц в разрядном срезе, рассматривать в виде последовательности цифр позиционного кода с предполагаемым переносом из младших разрядов.

Пусть в первом разрядном срезе – старшем разрядном срезе многорядного кода получено значение S_1, которое необходимо представить в заданной разрядной сетке многорядного кода одинаковыми количества Е. Для того , чтобы определить значение Е, необходимо решить следующее уравнение:

$$S_1 = E* 2^0 + E* 2^{-1} + E* 2^{-2} + E* 2^{-3} + E* 2^{-4} + ...E* 2^{-n},$$

где n– разрядность.

Для вычисления Е для любого разрядного среза следует решить уравнение

$$S_k = 2^{k-1}*E + ... + E* 2^0 + E* 2^{-1} + E* 2^{-2} + E* 2^{-3} + E* 2^{-4} + ...+ E* 2^{-n+k-1}$$

где последний член уравнения $E* 2^{-n+k-1}$ зависит от расположения разрядного среза, в котором задано количество единиц.

Представленный метод определяет преобразование нескольких операндов в уплотненный код, формирование уплотненного кода для одного операнда выполняется с попуском нескольких этапов.

Используя прием преобразования двоичного кода в уплотненный код, получаем структуру в которой двоичный операнд **000***…..0000*0*00* - где * - символы единиц заменен последовательностью: CCCCCC……..CCC, где С – цифра, соответствующая позиционному коду заполнения разрядной сетки.

Причем количество символов С может быть равно или меньше первоначальной разрядности операнда. Следующим этапом преобразования, согласно коду «-1» и разрядно-логарифмического кодирования, определяем структуру из следующих объектов:

DF(NF)DS(NS) - где DF- код , соответствующий позиционному разложению, NF - код позиции DF, DS - код, вычитаемый из DF(NF), NS – код позиции DS.

Для примера рассмотрим преобразование кода 101101. Такой код не является уплотнённым, поэтому вначале преобразуем в соответствии с квазиграфическим преобразованием: 1011101 =0211101=03333 +1 и далее в соответствии с кодом «-1» 6(3)2(0).

Реализация преобразования данных в предлагаемый формат включает небольшой набор операций и может быть реализована как дополнительная специализированная структура в составе процессора.

УДК 004.942(043.2)

В. В. Горіна, асистент,
О. М. Зудов, к.т.н., доцент
Національний авіаційний університет, Київ

КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ РОБОТИ ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ В УМОВАХ ЗАВАД

Канал зв'язку із шумами модулюється звичайним суматором, який додає до модульованого сигналу адитивний білий гаусів шум (АБГШ). Шумоподібний сигнал задається як масив випадкових чисел, що зберігається в окремому зовнішньому файлі і може бути створений за допомогою генератору випадкових чисел із нормальним розподілом. Співвідношення сигнал/шум можна регулювати як за допомогою вагових коефіцієнтів суматора, так і за допомогою дільника напруги. Останній спосіб дає змогу змінювати співвідношення сигнал шум прямо під час симуляції, використовуючи спеціально призначені «гарячі клавіші» для зміни опору потенціометра дільника напруги, що регулює поданий на суматор рівень шуму. Кореляційний приймач має стандартну структуру, що складається із перемножувача, інтегратора і порогового пристрою; для спрощення схеми синхронізація забезпечується штучно за допомогою пристрою синхронізації, що керується генератором повідомлення передавача. Сигнал із виходу порогового пристрою подається на пристрій неспівпадіння, другий вхід якого під'єднаний до генератору повідомлення передавача. Кількість неспівпадінь реєструється лічильником. За допомогою розробленого комп'ютерного симулятора можна досліджувати потенційну завадостійкість цифрових телекомунікаційних систем. У якості базової навчальної задачі можна будувати залежність ймовірності помилки від співвідношення Eb/No (відношення енергії одного біта до спектральної щільності шуму) і порівнювати її з теоретичною функцією, яка для варіанта модуляції BPSK як відомо задається виразом [2]:

$$P_b = \frac{1}{2} erfc\left(\sqrt{\frac{Eb}{No}}\right), \qquad (1)$$

де erfc(..) – компліментарна функція помилки. У варіанті M-PSK (фазова маніпуляція вищих порядків) даний вираз приймає вигляд:

$$P_e = erfc\left(\sqrt{\frac{Es}{No}\cdot sin\left(\frac{\pi}{M}\right)}\right), \quad (2)$$

де Es – енергія бітів символу, M – кількість символів у такті.

Для експериментальної оцінки ймовірності помилки необхідно запустити симуляцію декілька разів за різного співвідношення сигнал/шум. Отриманий процент помилкових бітів кожного разу буде давати статистичну оцінку ймовірності бітової помилки (BER). Проведені багатократні дослідження показали непогану узгодженість експериментальних результатів із теоретичними розрахунками.

Модель передавача забезпечує генерацію бінарного потоку, що задає повідомлення і модулює синусоїдальну несучу. У найпростішому варіанті використовується бінарна фазова маніпуляція (BPSK), але передавач можна переналаштувати на інші стандарти модуляції, зокрема на QAM і PSK вищих порядків.

Модель реалізовано у вигляді проекту в середовищі National Instruments Multisim [1]. Система складається із передавача, моделі каналу зв'язку із шумами, кореляційного приймача, пристрою синхронізації і лічільника помилок.

Розроблено симулятор роботи цифрової телекомунікаційної системи, а також змодельовано проходження сигналу по каналу із шумами. Розроблена комп'ютерна модель може бути використана як у навчальних цілях, так і для проведення наукових досліджень.

Розроблена модель дає змогу робити порівняльну характеристику різних телекомунікаційних систем, змінюючи стандарти модуляції, бітрейт та інші параметри. Для більш складних досліджень у схему може бути додані фільтри, які можуть змінювати спектральні характеристики шуму, зокрема, моделювати вузькосмугову заваду. Також можливо моделювання наприклад нестаціонарної завади.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Хернитер М. Е. Электронное моделирование в Multisim . Пер. с англ. – М.: ДМК Прес, 2010. — 578 с.

2. John G. Proakis, Masoud Salehi. Digital Communications. 5-th edition. – McGraw Hill Higher Education, 2008. – 1170 p.

УДК 004.42(043.2)

В. В. Горіна, асистент,
Н. О. Рибасова, асистент
Національний авіаційний університет, Київ

ОСОБЛИВОСТІ ПРОЕКТУВАННЯ ТА СТВОРЕННЯ ВЕБ-ЗАСТОСУВАННЯ

З появою веб-технології комп'ютер починають використовувати абсолютно нові верстви населення. Можна виділити дві найбільш характерні групи, що знаходяться на різних соціальних полюсах, які були стрімко залучені в нову технологію. З одного боку, представники елітарних груп суспільства – керівники великих організацій, президенти банків, топ-менеджери, впливові державні чиновники і т.д. З іншого боку, представники найширших верств населення – домогосподарки, пенсіонери, діти.

Спектр соціальних груп, що підключаються до мережі Інтернет і тих, що шукають інформацію, весь час розширюється за рахунок користувачів, що не відносяться до категорії фахівців в області інформаційних технологій. Це лікарі, будівельники, історики, юристи, фінансисти, спортсмени, мандрівники, священнослужителі, артисти, письменники, художники. Список можна продовжувати безкінечно. Той, хто відчув корисність і незамінність Мережі для своєї професійної діяльності або захоплень, приєднується до величезної армії споживачів інформації у «Всесвітній Павутині».

Веб-технологія повністю перевернула наші уявлення про роботу з інформацією, та й з комп'ютером взагалі. Виявилося, що традиційні параметри розвитку обчислювальної техніки – продуктивність, пропускна здатність, ємність запам'ятовуючих пристроїв – не враховували головного «вузького місця» системи – інтерфейсу з людиною. Застарілий механізм взаємодії людини з інформаційною системою стримував впровадження нових технологій і зменшував вигоду від їх застосування. І тільки коли інтерфейс між людиною і комп'ютером був спрощений до природності сприйняття звичайною людиною, послідував безпрецедентний вибух інтересу до можливостей обчислювальної техніки.

Для створення сайту використовують різні засоби: редактори тексту типу Блокнот, візуальні редактори типу Microsoft FrontPage, Macromedia Dreamweaver і безліч інших редакторів, а також конструктори сайтів (дизайнери). Конструктори веб-сайтів розміщуються на деяких сайтах в мережі Інтернет.

Веб-розробка – процес створення веб-сайту або веб-застосування. Основними етапами процесу є веб-дизайн, верстка сторінок, програмування для веб на стороні клієнта і сервера, а також конфігурація веб-сервера.

Залежно від поточного завдання, деякі етапи можуть бути відсутніми, або бути тісно пов'язані один з одним.

Важливою частиною проектування ресурсу останнім часом, стало приведення ресурсу у відповідність стандартам W3C, що забезпечує доступність змісту для людей з обмеженими фізичними можливостями та користувачів портативних пристроїв, а також кросплатформеність верстки ресурсу [2]. Також безпосередньо з дизайном сайтів суміжні маркетинг в Інтернеті (інтернет-маркетинг), тобто просування і реклама створеного ресурсу, пошукова оптимізація.

Залежно від розв'язуваних завдань для створення сайту вибирають ту чи іншу мову серверних скриптів. Для створення малих і середніх інтерактивних сайтів доцільно застосувати мова сценаріїв PHP [3]. Конкурентами PHP є технології ASP, JSP, Cold Fusion, Perl. Гідністю мови PHP є те, що він є безкоштовним, має відкриті вихідні коди і працює майже на всіх платформах.

Для створення (розробки) і супроводу динамічних сайтів використовують CMS (Content Management System) - Систему управління сайтом, яку називають движком сайту. В даний час популярними системами управління є Drupal, Joomla та WordPress. На основі цих CMS можна створювати функціональні і легко керовані PHP-сайти. Движки для Drupal, Joomla та WordPress є безкоштовними. Засоби розробки сайтів забезпечують поділ змістовної частини (контенту) від дизайну (шаблону веб-сторінки), що дозволяє змінювати зміст веб-сторінок, не зачіпаючи їх дизайну і змінювати шаблон сайту не зачіпаючи змісту його сторінок.

УДК 681.3.06

В. В. Демчик,
О. В. Корочкін, к.т.н.,
О. В. Русанова, к.т.н.,
Національний технічний університет України "КПІ ім. І. Сікорського", Київ

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ВИКОРИСТАННЯ ДРІБНОЗЕРНИСТОГО ПАРАЛЕЛІЗМУ В БАГАТОЯДЕРНИХ КОМП'ЮТЕРНИХ СИСТЕМАХ

В роботі досліджуються питання підвищення ефективності обчислень в багатоядерних комп'ютерних системах (БКС) за рахунок застосування дрібнозернистого паралелізму.

Програмування для БКС пов'язано з використанням концепції потоків, в якій програма представляється як набір паралельних легких процесів. Як правило, потоки реалізують обчислення в рамках середнього або крупнозернистого паралелізму. При цьому виникає проблема організації взаємодії потоків, пов'язана з вирішенням задач взаємного виключення і синхронізації, для вирішення яких в БКС використовуються спеціальні низькорівневі примітиви: семафори, атомік змінні, м'ютекси, події, критичні секції, монітори. Зі зростанням кількості ядер в БКС з'являється можливість зниження розміру зернистості паралелізму, на основі якого можна знизити складність задачі взаємодії потоків, а також спростити (автоматизувати) процес її вирішення. Сучасні мови та бібліотеки паралельного програмування наряду з засобами створення потоків та організації їх взаємодії містять інструменти і для підтримки дрібнозернистого паралелізму [1].

Бібліотека OpenMP. Дрібнозернистий паралелізм в бібліотеці можна реалізувати за допомогою набору прагм, пов'язаних з паралельним виконанням циклів. Прагма omp for дозволяє розбити тіло циклу на частини, виконання яких треба здійснити паралельно. Опція schedule дозволяє керувати розміром зерна паралелізму, а також вибирати вид алгоритму планування. Взаємодія потоків здійснюється через бар'єрну синхронізацію.

Мова C#. Засоби реалізації дрібнозернистого паралелізму пов'язані з статичним класом Parallel, методи якого Parallel.For, Parallel.ForEach дозволяють реалізувати паралельне виконання циклів, а за необхідністю з контролем та керуванням станом циклів, 64-розрядними індексами та локальними даними потоку. В

цьому ж класі реалізований метод Parallel.Invoke, який виконує всі надані йому дії, за можливістю в паралельному режимі. Мова Java. Засоби реалізації дрібнозернистого паралелізму пов'язані з моделлю fork-join, яка базується на алгоритмі "розділяй та владарюй" [2].

Модель fork-join підтримує декілька стилів ForkJoinTasks: клас RecursiveAction забезпечує стиль паралельного рекурсивного розкладання для задач, що не повертають результат, клас RecursiveTask - для задач, що повертають результат.

В роботі виконано дослідження ефективності розглянутих методів і засобів реалізації дрібнозернистого паралелізму в БКС. Для цього був розроблений пакет програм для матричних операцій з використанням бібліотеки OpenMP, мов C# та Java. Кожна операція реалізовувалась у вигляді чотирьох програм П1-П4. В програмі П1 використовувався традиційний підхід, який базується на програмуванні чотирьох потоків та низькорівневих примітивів їх взаємодії (крупнозернистий паралелізм), в програмі П2 – розпаралелювались тільки цикли (дрібнозернистий паралелізм), в програмі П3 – використовувались потоки, в яких обчислення додатково проводяться з розпаралелюванням циклів. Програма П4 являла собою послідовну реалізацію, необхідну для розрахунку коефіцієнтів прискорення.

Проведено дослідження часу виконання програм пакету в реальній чотирьох ядерної БКС в залежності від розмірності задач, кількості використовуваних ядер, зернистості паралелізму.

Результати експериментів показали можливість скорочення часу вирішення розглянутих задачі за рахунок використання тільки дрібнозернистого паралелізму, а також як складової частини крупнозернистого паралелізму.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Эхтер Ш., Робертс Дж. Многоядерное программирование. — СПб.: Питер, 2010. — 316 с.

2. Lea, Doug. A Java Fork/Join Framework, In Proceedings of ACM Java Grande 2000 Conference (San Francisco, California, June 3-5, 2000)

УДК 004.7 (043.2)

В. І. Дрововозов, к.т.н., доцент
Н. В. Журавель, асистент
Национальный авиационный университет, Киев

ПІДВИЩЕННЯ НАДІЙНОСТІ ЗВ'ЯЗКУ В ЛОКАЛЬНИХ БЕЗДРОТОВИХ МЕРЕЖАХ

Проблема необхідності значного збільшення швидкості передачі даних і підвищення якості обслуговування користувачів (зменшення ймовірності помилки передачі інформації) дуже актуальна в бездротових системах зв'язку, що працюють в складних умовах поширення сигналів. Зменшення помилок передачі інформації - один із шляхів вирішення даної проблеми. Це зменшення можна істотно здійснити за допомогою рознесеного прийому або передачі сигналів кількома антенами, відстань між якими вибирається таким, щоб забезпечити слабку кореляцію завмирань сигналів в цих антенах.

В сучасних бездротових мережах все більше застосування знаходять методи радіодоступу. В даний час, в використовуваних протоколах (наприклад, 802.11x) передбачені заходи щодо забезпечення надійності прийому радіосигналів в умовах багатопроменевого поширення радіохвиль: методи передачі по паралельних каналах, блочного кодування та ін. Однак, передбачені заходи захисту не є абсолютними. Тому доцільно доповнити їх такими, які не вимагають зміни прийнятих протоколів. Одним із шляхів такого підходу є застосування просторово-часового методу, заснованого на використанні цифрового діаграмостворення (ЦДС) на базі цифрових антенних решіток (ЦАР), використання яких має безперечну перевагу в порівнянні з традиційними антенами досягненням високої перешкодозахищеності ліній зв'язку, стійкого функціонування при багатопроменевому поширенні радіохвиль і впливі активних перешкод штучного походження. Використання адаптивних приймально-передавальних ЦАР дозволяє реалізувати одночасний прийом безлічі сигналів в широкому просторовому секторі з подальшим вимірюванням параметрів кожного з них. Високої завадостійкості систем зв'язку з ЦАР сприяє також цифрове формування високоідентичних частотних фільтрів в прийомних

каналах з гранично малим розкидом їх амплітудно-частотних і фазочастотних характеристик.

ЦАР є більш досконалою системою, в якій гранично повно можна реалізувати адаптивні методи обробки сигналів.

Переваги систем з використанням ЦДС на базі ЦАР відомі досить добре. Завдяки ЦДС робота радіоканалів при багатопроменевому поширенні радіохвиль стає більш надійною.

У разі прийому багатопроменевого сигналу однією антеною, усунення впливу короткочасного завмирання можливо, наприклад, за рахунок методів блокового кодування. Однак, при повному зникненні сигналу такі методи можуть виявитися неефективними. Інша картина спостерігається при використанні декількох антен. Цей варіант відповідає обробці сигналів в MIMO-системі (Multiple-Input Multiple-Output).

Застосування ЦАР з MIMO-системою дозволяє вирішити проблему стійкого функціонування систем зв'язку в умовах впливу активних завад, багатопроменевого поширення радіохвиль і пов'язаних з ним явищ. Пропонується застосовувати MIMO-системи з використанням механізму просторово-часової обробки (Space-Time Processing - STP) сигналів. Система з M передавальних і M приймальних антен здатна забезпечити пікову пропускну здатність теоретично в M разів більшу, ніж звичайні системи досягненням розбиття передавачем потоку даних на незалежні послідовності бітів та пересиланням їх одночасно використанням масиву антен.

Виконано вибір підходу до вирішення завдання оцінки параметрів просторового спектра сигналу, прийнятого декількома приймальними антенами. Процедура знаходження оптимальної оцінки може здійснюватися з використанням відповідних методів нелінійного програмування, наприклад, градієнтним методом. При цьому на кожному черговому кроці за рахунок поновлення даних критеріальна функція зменшується, сходячись до найменшого значення. [1]

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Ермолаев В.Т. Адаптивная пространственная обработка сигналов в системах беспроводной святи / В.Т. Ермолаев, А.К. Флаксман. «Нижний Новгород», 2006. – 3 с.

УДК 004.056.53(043.2)

О. В. Дубчак,
Я. С. Мазур
Національний авіаційний університет, Київ

ПРОТОКОЛИ ТЕХНОЛОГІЇ VoIP

Клієнт-серверна технологія VoIP (Voice over Internet Protocol) або IP-телефонія на даний час набула значного розповсюдження. Ефективність технології VoIP, що використовує мережу з пакетною комутацією, визначається способом передавання пакетів середовищем, яке розподіляється, - загальним каналом передачі даних, що дозволяє заощаджувати фінансові ресурси. Будь-який пристрій, який має змогу приймати голосовий сигнал та відтворювати отриманий голосовий трафік, може бути клієнтом VoIP.

Якість передавання даних залежить від VoIP – провайдера та способу підключення до Internet.

Відсутність в технології VoIP штатних механізмів гарантування достатнього рівня інформаційної безпеки призводить до загострення проблеми захисту інформації в такій мережі відповідно до цілей та моделі загроз.

Питання убезпечення інформації в технології VoIP можна вирішити шляхом використання спеціальних протоколів захисту інформації, таких як TLS (Transport Layer Security) або VPN (Virual Private Network), а також додаткових протоколів, таких як SIP (Session Initiation Protocol) та H.323.

Протокол TLS є наступним поколінням поширеного криптографічного протоколу SSL (Secure Sockets Layer), який базується на асиметричній криптографії.

Усі додаткові протоколи захисту інформації в технології VoIP можна розподілити на два види: *відкриті,* до яких можна віднести відомі міжнародні специфікації та стандарти; *закриті* – протоколи VoIP, у яких інформація щодо структури повідомлень не розголошується.

Протокол H.323 відомий як один з перших протоколів, який відповідав вимогам систем стандартної телефонії та визначав набір правил передавання звукових і відеоданих комп'ютерними мережами, що визначило його як інтегрований набір протоколів

для одного застосування. Архітектура протоколу H.323 монолітна, містить три основні складові, і для створення нової послуги може знадобитися модифікація кожної із цих складових.

Більшість сучасних світових операторів VoIP для передавання голосових даних у мережах з пакетною комутацією використовують відкритий протокол встановлення сесії SIP, який забезпечує ініціювання, контроль та ліквідацію сеансу обміну інформацією. Разом із цим протоколом використовують протокол SDP (Session Description Protocol - протокол опису сеансу), оскільки SIP власне не передає інформацію. Протокол SIP використовує текстовий формат повідомлень, подібно протоколу HTTP. Це полегшує синтаксичний аналіз, генерацію коду та експлуатаційне керування, дозволяє реалізувати протокол на базі будь-якої мови програмування, дає можливість ручного уведення деяких полів, а також спрощує аналіз повідомлень.

Слід відзначити також деякі властивості протоколу SIP, що свідчать на його користь:

– *багатоадресне розсилання інформації* використовується протоколом SIP для перенесення сигнальних повідомлень, а не лише для доставки мовної інформації, як у протоколі H.323; користувач SIP-мережі може реєструвати декілька своїх адрес і вказувати пріоритетність обслуговування кожної з них;

– *персональна мобільність користувачів* протоколом SIP підтримується гнучкіше;

– *масштабованість мережі*: сервер SIP може обробити більше викликів ніж H.323, оскільки за вмовчання не зберігає відомостей про поточні сеанси зв'язку;

– *час установлення з'єднання* SIP за рахунок використання протоколів TCP і UDP значно менший відносно такої ж характеристики протоколу H.323, в якому необхідно здійснювати обмін повідомленнями кілька разів, а у протоколі SIP потрібна одна транзакція, що скорочує витрати часу на встановлення з'єднання.

Отже, SIP характеризується відносною простотою архітектури, меншим часом встановлення з’єднання, реалізацією додаткового функціоналу, невисокою вартістю, відносною простотою взаємодії із засобами безпеки, можливістю бути використаним для зв'язку з інтелектуальними мережами.

УДК 004.75

О. О. Жолдаков,
А. О. Жолдаков
Національний авіаційний університет, Київ

АНАЛІЗ ПРОБЛЕМИ ФОРМУВАННЯ МІНІМАЛЬНОГО ПЕРЕЛІКУ ОБЛАДНАННЯ ПОВІТРЯНИХ СУДЕН, ЩО ЗАБЕЗПЕЧУЄ БЕЗПЕКУ ТА РЕГУЛЯРНІСТЬ ПОЛЬОТІВ

Останнім часом питанням льотної придатності та безпеки проведення польотів приділяється все більше уваги, що пов'язано із посиленням вимог *ICAO* та МАК до міжнародних авіаперевезень та організації безпечного єдиного авіаційного простору. Обов'язковою вимогою є дотримання встановлених міжнародних вимог всіма країнами, членами *ICAO*.

Цілями системи підтримання льотної придатності є: забезпечення безпеки польотів не нижче досягнутого світового рівня; зниження витрат на експлуатацію повітряних суден.

Перспективним напрямком зниження витрат являється розробка і впровадження допустимих обмежень на наявність і працездатність компонентів повітряних суден.

Конструкція сучасних повітряних суден (ПС) передбачає наявність високонадійного обладнання і системного резервування. Практика експлуатації ПС показує, що на обмежений період часу робота всіх елементів систем не є обов'язковою, якщо забезпечується прийнятний рівень безпеки. Виходячи з цього, для підвищення ефективності використання ПС в практику експлуатації вводяться нормативні документи, що дозволяють при необхідності тимчасово здійснювати безпечні польоти з несправним (незадіяним) обладнанням.

Такими нормативними документами є «Мінімальні переліки обладнання» (в зарубіжній практиці *MMEL* і *MEL*). *MMEL* (*Master Minimum Equipment List*) – Основний мінімальний перелік обладнання (далі – Основний перелік), що розробляється фірмою для типу ПС; *MEL* (*Minimum Equipment List*) – Мінімальний перелік обладнання (далі – Перелік), що розробляється експлуатантом для кожного типу ПС. Цими документами санкціонуються деякі відхилення від вимог сертифіката типу, для того щоб забезпечити регулярну експлуатацію ПС. Ці умовні

відхилення інакше називають як «умови допуску до експлуатації (виконання польотів)».

Основним завданням Переліку *MEL* є встановлення для експлуатанта балансу між прийнятним рівнем безпеки польотів та рентабельністю ПС при його експлуатації з частково несправним обладнанням. Перелік *MEL* дозволяє експлуатантам більш оперативно організовувати експлуатацію (польоти) ПС і уникати зайвих затримок або скасування рейсів, не ставлячи під загрозу безпеку польотів у випадках, коли ПС допускається до польотів з несправним (незадіяним) обладнанням.

Як Основний перелік, так і Перелік *MEL* затверджуються і приймаються повноважним органом контролю льотної придатності. Вони складаються з переліків компонентів і систем, яким присвоюється статус «Допускається», «Допускається, якщо» або «Не допускається» в залежності від їх впливу на безпеку польотів. Компоненти зі статусом «Допускається» або «Допускається, якщо» можуть залишатися в несправному стані протягом обмеженого періоду часу.

Метою Основного переліку є надання експлуатантам ефективного і надійного засобу для швидкого визначення того, чи може ПС бути допущено до польоту, не ставлячи під загрозу його безпеку.

Перелік є похідним від Основного переліку і застосовується конкретним експлуатантом з урахуванням особливостей застосовуваних робочих процедур і реальних умов експлуатації. Будучи затвердженим і допущеним до використання, Перелік дозволяє здійснювати експлуатацію обладнання, що знаходиться в неробочому стані.

Робота над Основним переліком ґрунтується на глибокому аналізі надійності компонентів і систем ПС, визначенні повного переліку можливих функціональних відмов і ступеня небезпеки ситуацій. При цьому робота над Переліком *MEL* ґрунтується перш за все на Основному переліку *MMEL*, а також на знанні фактичних характеристик парку ПС експлуатанта, їх конфігурації, умов і досвіду експлуатації.

Застосування Переліку *MEL* дає можливість експлуатанту дотримуватися вимог по регулярності польотів, забезпечувати прийнятний рівень безпеки і скорочувати експлуатаційні витрати.

УДК 519.852.35:004.7

І. А. Жуков, д.т.н.
М. К. Печурін, д.т.н.
Національний авіаційний університет, Київ,Україна,
Л. П. Кондратова, к.т.н.
Інститут прикладного системного аналізу КПІ ім. І. Сікорського, Київ,Україна,
С. М. Печурін, к.т.н.

БАЛАНСУВАННЯ РОЗПОДІЛЕНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ПАРАЛЕЛЬНОЇ КЛАСИФІКАЦІЇ ОБ'ЄКТІВ

Інформаційна технологія класифікації об'єкту (-тів) може бути реалізована у вигляді розподіленої комп'ютерної мережі, організованої для одночасного (паралельного) розв'язання цієї задачі. Така інтегрована інформаційна система суть гетерогенний кластер, включає в себе інтелектуальні сенсори (відеокамери, камери відеоспостереження, тепловізори тощо) [1] з комп'ютерами, об'єднаними телекомунікаційною мережею. Велика кількість об'єктів, що надходять (буквально, якщо мова йде про пасажирів метрополітену) для класифікації, різна (обчислювальна) потужність комп'ютерної техніки і пристроїв зв'язку, різноманітність застосованих алгоритмів класифікації (рухомих, статичних об'єктів) та інтелектуальних сенсорів призводить до необхідності балансування (узгодження) параметрів компонентів комп'ютерної мережі паралельної класифікації об'єктів.

Розв'язання проблеми балансування є дуже важливим з урахуванням показника «витрати - ефективність», який для сучасних застосувань звучить як «втрати - неточність класифікації». Задача полягає у розподілі інформаційних та обчислювальних ресурсів комп'ютерів та компонентів системи зв'язку, що споживаються для (паралельної) обробки потоків фото- та відеокадрів, що отримано від інтелектуальних сенсорів, з метою оптимальної класифікації визначеного об'єкту.

Планування інформаційних та обчислювальних ресурсів, що споживають у мережі, виконується за показником «витрати - ефективність». Інтеграція інформаційних, обчислювальних та телекомунікаційних потужностей для розв'язання задачі

класифікації надає нові можливості покращання показника ефективності тільки за умови збалансованості розподіленої мережі, тобто відсутності вузьких місць і недозавантажень потужностей.

Для балансування розподіленої комп'ютерної мережі паралельної класифікації об'єктів пропонується модель, подібна до запропонованої у [2].

Відомо матрицю A, елемент a_{ij} якої визначає об'єм (інформаційного, обчислювального, телекомунікаційного) ресурсу інтелектуального сенсора з комп'ютером i, що витрачається на обробку вибірки, яка представляє пред'явлений інтелектуальному сенсору j для класифікації об'єкт; x_j - кількість об'єктів, що пред'являються інтелектуальному сенсору для класифікації з комп'ютером j.

Основна частина моделі для визначення параметрів збалансованої розподіленої комп'ютерної мережі паралельної класифікації об'єктів синтезована на основі класичної моделі В.Леонтьєва [3] і має вигляд: $X - A \cdot X = 0.$

Сформовані додаткові обмеження і цільова функція призводять до спеціальної моделі, для якої застосовано відповідний метод (Нелдера – Міда) нелінійного програмування для визначення параметрів A, X .

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Войтович І.Д., Корсунський В.М. Інтелектуальні сенсори. К.: Інститут кібернетики ім. В.М.Глушкова, 2007. – 514с.

2. Жуков И.А., Печурин Н.К., Кондратова Л.П., Печурин С.Н. Распределение ресурсов в вычислительном кластере для БПЛА // Проблеми інформатизації та управління: зб. наук. праць.−2016.− Вип.3 (55).− С. 1-5.

3. Леонтьев В.В. Межотраслевая экономика. − М.: Экономика, 1997. − 315 с.

УДК 004.056.5(043)

Б. Е. Журиленко, к.ф.-м.н.
Национальный авиационный университет, Киев

МОДЕЛИРОВАНИЕ ПРОЦЕССА ВЗЛОМА И АНАЛИЗА РАБОЧЕГО СОСТОЯНИЯ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Проектирование и разработка системы технической защиты информации (ТЗИ), в общем-то, требует экспериментальных проверок и исследований по определению возможностей защиты информации спроектированных и разработанных ТЗИ. В настоящее время экспериментальные исследования в большинстве случаев проводятся только при сертификации защиты. Причем, оценка возможностей защиты представляет собой достаточно сложную задачу. Трудности экспериментальных проверок ТЗИ заключаются в том, что реальные результаты взлома защиты становятся известны только после ее реального взлома. Для того чтобы сделать сравнительные исследования и заключения по возможностям той или иной защиты информации, необходимо провести реальный взлом ТЗИ и одновременно получить ее количественную оценку, например, ее вероятность взлома. Естественно, ТЗИ могут попытаться взломать при ее сертификации и не факт, что при этом защита будет реально взломана. С другой стороны, разработчику защиты важно знать вероятность взлома защиты информации на каждом этапе ее работы и желательно из реальных попыток взлома. В этом случае, зная в каждый момент времени по исходным данным вероятность взлома работающей ТЗИ, разработчик сможет оценить вероятность возможного взлома защиты по реальным параметрам попыток взлома, которые можно получить всегда, например, по количеству попыток и времени этих попыток взлома. Эти результаты помогут разработчику принять решение о замене используемой ТЗИ или ее модернизации, что позволит сэкономить финансовые и материальные ресурсы, вкладываемые в защиту информации. Проверить возможности ТЗИ и провести экспериментальные исследования той или иной защиты можно, если смоделировать процесс взлома соответствующий реальным физическим условиям. В связи с этими задачами, целью данной работы являлась разработка методологии экспериментальных исследований и оценки вероятности взлома

или защиты ТЗИ по параметрам, которые моделируются в соответствие с реальными физическими условиями процесса взлома. В результате выполненной работы были сделаны следующие выводы. Показана возможность моделирования процесса взлома ТЗИ в простейшем случае и методология анализа рабочего состояния ТЗИ, которая позволяет по направлению и статистики серий данных взлома провести анализ состояния ТЗИ. Если направление взлома и параметры серии попыток взлома будут меняться в процессе эксплуатации ТЗИ, то ее параметры и состояние защиты можно будет корректировать. После анализа состояния и определения параметров защиты информации возникает возможность сравнения параметров проектируемой ТЗИ и ее рабочего состояния по результатам анализа попыток взлома. Если по результатам выполненного анализа состояние ТЗИ на данный момент близко к параметрам проектируемого или возможности взлома, то проектировщик может провести модернизацию или ее замену. Результаты исследования моделирования процесса взлома могут быть использованы и злоумышленником для анализа состояния защиты. По полученным параметрам взлома ТЗИ злоумышленник может сориентироваться в правильном ли направлении идет процесс взлома и при каких условиях будет достигнут нужный для него результат. Однако следует заметить, что проектируемые параметры ТЗИ злоумышленник знать не будет. При необходимости он может изменить направление взлома для достижения оптимального направления и, следовательно, нужного результата, но это не значит, что взлом идет в правильном направлении, заложенном организатором защиты информации. С точки зрения защиты информации организатор защиты тоже может и должен знать результаты направления взлома и анализа состояния работающей ТЗИ, которые можно сравнить с реальными исходными планируемыми параметрами ТЗИ и в случае необходимости вовремя провести модернизацию защиты в нужном направлении. Таким образом, организатор защиты может контролировать ее состояние в процессе работы ТЗИ. С другой стороны, если злоумышленник после анализа состояния работающей ТЗИ может увидеть, что для ее взлома понадобится много времени и финансовых затрат, то он может отказаться от взлома данной ТЗИ.

УДК 004.007.5(32.323.1)

Р. В. Зюбіна,
Ю. М. Бабенко
Національний авіаційний університет, Київ

ОСОБЛИВОСТІ ІДЕНТИФІКАЦІЇ ЛЮДИНИ НА БАЗІ ГОЛОСОВОЇ БІОМЕТРІЇ

Стрімкий розвиток сучасних інформаційних технологій ставить нові задачі в процесі створення надійних систем захисту інформаційних ресурсів. Все більшого поширення набувають системи біометричної ідентифікації людини, серед яких найпопулярнішими є системи, що базуються на аналізі відбитків пальців, сітківки ока, ДНК, складу крові, ритму серцебиття, структурі волосся та інші. В процесі аналізу характеристик голосу людини важливу роль відіграють і регіональні особливості складу мови, акценту, діалекту людини. Голосова ідентифікація має суттєву відмінність порівняно з багатьма іншими методами ідентифікації - її можна провести віддалено, по телефону. Це може бути дуже важливо, наприклад, при розслідуванні злочину, коли є запис голосу підозрюваного, який в подальшому може бути використаний для підтвердження, або спростування виконаних ним злочинних дій.

Унікальність голосових характеристик людини зумовлена великою кількістю фізіологічних особливостей, таких як будова голосових зв'язок, об'єм легень, будова трахеї, носоглотки, розташування зубів. Однак, на сьогодні, недосконалість існуючих систем звукозапису значно ускладнює процес точної ідентифікації людини за голосом та робить актуальним питання правильного прийняття рішення в умовах коли шум значно перевищує корисний сигнал.

Виділяють дві групи мовних звуків – голосні (тони, або вокалізовані звуки), які в свою чергу становлять вагомий інтерес в процесі ідентифікації, та приголосні (шуми з незначним додаванням тону). Вокалізовані звуки утворюються наступним чином: потік повітря з легень проходить через голосову щілину, яка періодично замикається, виробляючи звукові імпульси. Період, з яким виробляються імпульси, називають періодом основного тону. Далі поширення імпульсів відбувається через ряд порожнин,

які впливають на частотний склад результуючого сигналу. Розмір і форма порожнин мовного тракту можуть бути використані в якості індивідуальних характеристик людини в процесі ідентифікації за голосом[1].

Існуючі методи ідентифікації можна розділити на три основні групи в залежності від області в якій вони працюють:

1. Часова область (метод амплітудної селекції, метод автокореляції, метод максимальної правдоподібності, методі адаптивної фільтрації).
2. Частотна область (спектральний гармонічний метод, метод кепстрального аналізу, метод максимальної правдоподібності та інші).
3. Метод оснований на фізіології слухового апарату (рецепторний метод).

Методи, що працюють в часовій області відрізняються простотою реалізації, а ті що працюють в частотній, в свою чергу, дають можливість більш точного визначення основних характеристик голосової біометрії.

На сьогодні при визначенні частоти основного тону, як основної характеристики в процесі ідентифікації голосу людини, виникає ряд проблем, а саме [2]:

- складність реалізації алгоритмів визначення частоти основного тону;
- низька ймовірність визначення;
- помилки у процесі визначення;
- низька стійкість алгоритму до зовнішніх змін.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Первушин Е. А., Лавров Д. Н. Алгоритм извлечения признаков речевого сигнала во временной области для задачи распознавания дикторов //Вестник Омского университета. – 2011. – №. 2.

2. Жиляков Е. Г., Фирсова А. А., Чеканов Н. А. Алгоритмы обнаружения основного тона речевых сигналов //Научные ведомости Белгородского государственного университета. Серия: Экономика. Информатика. – 2012. – Т. 21. – №. 1-1 (120).

УДК 656.71.0521

Н. П. Кадет, ст.викладач
Національний авіаційний університет, Київ
О. М. Башкиров, п.н.с.
ЦНДІ ОВТ ЗС України

ОЦІНКИ СТІЙКОСТІ ФУНКЦІОНУВАННЯ СИСТЕМИ ЗВ'ЯЗКУ В УМОВАХ НЕГАТИВНОГО ВПЛИВУ

Розглядаються питання моделювання функціонування системи зв'язку спеціального призначення в умовах ведення радіоелектронної боротьби та інших факторів негативного впливу.

Якість системи зв'язку визначається її готовністю, функціональною сумісністю, стійкістю, мобільністю, пропускною спроможністю та безпекою. Стійкість системи зв'язку характеризується її здатністю забезпечувати управління військами та зброєю в умовах дії усіх негативних чинників та вражаючих факторів. Згідно державного стандарту та керівних документів стійкість розглядається як інтегральна властивість, що обумовлюється її живучістю, завадостійкістю та надійністю. Вимоги до показників стійкості визначаються через показники живучості, надійності та завадостійкості системи зв'язку. У цей час використовуються методики оцінки ефективності систем зв'язку різних ієрархій та призначення, в тому числі для оцінки ефективності виконання окремих завдань. В роботі [1] розглянуто характер впливу навмисних завад на засоби радіозв'язку авіаційних засобів, проведений аналіз їх протирозвідкової захищеності в умовах РЕБ, одержані оцінки енергетичної скритності функціонування бортових засобів зв'язку з псевдовипадкового перестроювання робочої частоти. В роботах [2,3] розглядаються моделі для оцінки імовірнісного показника розвідзахищеності системи зв'язку. Комплексна оцінка стійкості функціонування системи зв'язку спеціального призначення в умовах ведення радіоелектронної боротьби у відомих джерелах відсутня, тому відомі моделі та методики потребують удосконалення, а розробка відповідної моделі є актуальним науковим завданням.

Розглядається модель оцінки розвідзахищеності системи зв'язку. Порушення процесу передавання інформації в системи зв'язку може проходити під впливом різних чинників, які можуть

діяти обмежено (на протязі хвилин, годин) або довготривало (десятки годин). Функціонування системи зв'язку з урахуванням цієї групи чинників можна розглядати як близький до стаціонарного, а їх вплив оцінювати імовірно-часовими характеристиками, які прийняті в теорії надійності. В якості основних показників оцінки стійкості системи зв'язку відносно даної групи чинників використовуються коефіцієнт справної дії та середній час справної роботи або простою, які відносяться до окремого елементу або напрямку зв'язку.

Удосконалення відомих моделей оцінки розвідзахищеності системи зв'язку проведено шляхом врахування того, що імовірність виявлення роботи передавача залежить від режиму його роботи, потужності випромінювання та дальності до станції розвідки. Аналогічні проблеми виникають при оцінці завадозахищеності засобів спеціального зв'язку. Сучасні комплекси і засоби зв'язку відрізняються універсальністю режимів роботи різноманітних засобів, що використовуються на різних рівнях управління, а також появою режимів функціонування, що спроможні забезпечувати зв'язок при рівні сигналу нижчому за рівень завад. Доповідається про розробку методики оцінки ефективності функціонування УКХ-радіомереж в умовах радіоелектронного подавлення.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Гепко І.О. Завадозахищеність бортових засобів радіозв'язку із псевдовипадковим перестроюванням робочої частоти. Збірник наукових праць наукового центру Повітряних сил ЗС України. – 2004. – № 7. – С. 57-62.

2. Борисов В.И. и др. Помехозащищенность систем радиосвязи с расширением спектра сигналов методом псевдослучайной перестройки рабочей частоты: Монография. – М., Радио и связь, 2000. – 384 с.

3. Скляр Б. Цифровая связь. Теоретические основы и практическое применение.: Пер. с англ. – М.: Издательский дом «Вильямс», 2003. – 114 с.

УДК 004 (043.2)

Р. М. Капорін,
А. В. Коган, к.т.н., асистент
Національний технічний університет України «КПІ ім. І. Сікорського», Київ

СПОСОБИ ОРГАНІЗАЦІЇ БАГАТОШЛЯХОВОЇ МАРШРУТИЗАЦІЇ

Розширення сфери застосування комп'ютерних мереж підвищує вимоги до якості передачі інформації (QoS) та її безпеки. Багатошляхова маршрутизація один з перспективних способів вирішення даного завдання.

Основною умовою організації безпечної багатошляхової маршрутизації є наявність достатньої кількості шляхів, необхідних для передачі даних і можливого обходу скомпрометованих мережевих пристроїв або тих пристроїв, що вийшли з ладу. Для цього в мережі необхідно сформувати множину шляхів, які не перетинаються 0, 0, що зменшить ймовірність прослуховування і прискорить процес передачі за рахунок використання декількох шляхів.

Використання багатошляхової маршрутизації передбачає ряд переваг, а саме:

- балансування навантаження;
- поліпшення показників якості обслуговування;
- підвищення рівня безпеки.

СПОСОБИ формування множини ШЛЯХІВ, що не перетинаються

Для організація безпечної багатошляхової маршрутизації в комп’ютерній мережі доцільно використовувати способи побудови множини шляхів, що не перетинаються, тобто не мають спільних вузлів.

Для вирішення поставленої задачі запропоновано використовувати модифікований алгоритм Беллмана-Форда та хвильовий алгоритм для формування декількох шляхів.

Модифікований алгоритм Беллмана-Форда

В результаті роботи алгоритму Беллмана - Форда 0 маємо на виході послідовність вершин через яких він пройшов, та вартість

даного шляху. За знайденими вершинами можна відтворити ребра, які були використані алгоритмом.

Ідея запропонованого модифікованого способу полягає у наступному: алгоритм шукає найкоротший шлях поміж початковою і кінцевою вершинами у графі, а потім видаляє усі вершини, що містяться у шляху і продовжує пошук нового шляху доти, доки ще є можливість з'єднати ці дві вершини. Так буде гарантовано знайдена множина шляхів з найменшими вартостями.

Модифікований хвильовий алгоритм

Для формування множини шляхів в роботі запропоновано модифікований хвильовий алгоритм, який формує відразу всю множину шляхів, що не перетинаються між двома точками.

Розглянемо на прикладі принцип роботи алгоритму. На першому етапі будується множина шляхів. Потужність такої множини є не більшою ніж кількість ребер, що виходять з початкової вершини, бо це максимальна кількість шляхів, що не будуть перетинатися. На наступному етапі утворюються хвилі, тобто обираються нові можливі кандидати для переходу. Спочатку обираються вершини, у яких найменша кількість вихідних з'єднань, бо інакше інша вершина може відрізати наступний крок для цієї, хоча вона б мала інші варіанти для переходу.

Виконання алгоритму продовжується поки є можливість утворення нових шляхів. В кінці роботи алгоритму буде отримано множину шляхів, що не перетинаються.

У даній роботі були запропоновані і обґрунтовані два модифікованих способи формування множин шляхів, що не перетинаються для організації багатошляхової маршрутизації. Основними ж критеріями при організації такої маршрутизації є безпека та якість обслуговування, досягти яких вдається за рахунок формування множини шляхів, що не перетинаються.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Thomas, T. M. (2000). *ICND: Interconnecting Cisco network devices*. New York: McGraw-Hill.

2. Cormen, T. H., Leiserson, C. E., & Rivest, R. L. (1990). *Introduction to algorithms*. Cambridge, MA: MIT Press.

УДК 004.42 (043.2)

Н. В. Кірхар, к.т.н.,
Д. В. Ходаков, к.т.н.
Національний авіаційний університет, Київ

ОСОБЛИВОСТІ ПРОГРАМУВАННЯ ПІД ANDROID

У мобільних технологій багатообіцяюча перспектива, і Android представляє собою життєздатну і цікаву для розробників платформу. Android – операційна система на основі ядра Linux з інтерфейсом користувача на основі прямого маніпулювання, призначена в першу чергу для сенсорних мобільних пристроїв, таких як смартфони і планшетні комп'ютери. Операційна система використовує сенсорне введення [2].

Версії ОС Android нумеруються в порядку зростання: 1.6, 2.0 т.д., остання 8.0. У них також є імена, відповідні назвам різних десертних страв: Donut («пампушка»), Eclair («еклер» або «глазур») і Oreo («Орео»).

Версії Android поділяються і за рівнями API, які позначаються зростаючими послідовними цілими числами. Так, Android API рівня 17 відноситься до версії Android 4.2, або Jelly Bean. Базовим елементом цієї операційної системи є реалізація Dalvik віртуальної машини Java, і все програмне забезпечення і застосування спираються на цю реалізацію Java.

Android забезпечує велике різноманіття додатків, що дозволяє створювати інноваційні програми та ігри для мобільних пристроїв в середовищі мови Java.

Офіційним середовищем розробки є Android Studio, створене на базі Intellij IDEA. Містить емулятор, засоби відлагодження, профілювання пам'яті та швидкодії. Також доступні плагіни для Intellij IDEA, Eclipse та NetBeans [1].

В Android можна запускати багато додатків. Але один з них є головним і займає весь екран. Від поточного додатка можна перейти до попереднього або запустити новий. Це схоже на браузер з історією переглядів.

Додаток Android можна уявити як набір завдань, кожна з яких називається діяльністю (activity). Activity – це центральний компонент платформи Android. Кожна activity являє собою задачу,

яку виконує застосування, вона часто пов'язана з певним екраном призначеного для користувача інтерфейсу [3].

Кожен екран користувача інтерфейсу представлений класом Activity в коді. Різні activity містяться в процесах. Activity може навіть жити довше процесу. Activity може бути призупинена і запущена знову зі збереженням всієї потрібної інформації, використовує спеціальний механізм опису дій заснований на Intent. Коли потрібно виконати дію (зробити дзвінок, надіслати листа, показати вікно), викликається Intent [1].

Також Android містить сервіси подібні демонам в Linux для виконання потрібних дій у фоновому режимі (наприклад, програвання музики). Для обміну даними між додатками використовуються Content providers (провайдери вмісту).

Усі файли ресурсів Android записуються у форматі XML, що дає змогу редагувати їх без встановлення спіального редактора.

Емулятор Android може використовуватися для виконання і налагодження додатків Android майже без необхідності використання реального пристрою.

Існує також безліч інших інструментів для взаємодії з мобільними телефонами і емуляторами в інтерфейсі командного рядка, а також спеціальні утиліти для розробки призначених для користувача інтерфейсів Android і стиснення додатків.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Рето Майер. Android 2. Программирование приложений для планшетных компьютеров и смартфонов. − М.: Эксмо, 2011. − 672 с.

2. Харди Б., Филлипс Б. Программирование под Android. Для профессионалов. − М.: Big Nerd Ranch, 2013. − 592 с.

3. Саид Хашими, Сатия Коматинени, Дэйв Маклин. Разработка приложений для Android. Для профессионалов. − М.: Питер, 2011. − 736 с.

УДК 004.047 (043.2)

Н. А. Ковалев, к.т.н.
Национальный авиационный университет, Украина

ОРГАНИЗАЦИЯ ЛОГИЧЕСКИХ ВЫЧИСЛЕНИЙ

Перспективные бортовые системы управления предполагают расширение и усложнение логических вычислений [1]. В этой связи перспективным видится применение аппарата позиционной алгебры логики (ПАЛ) [2]. В ней в отличие от булевой функции алгебры логики (ФАЛ) представляются и вычисляются на основе принципов позиционности посредством эквивалентных преобразований и позиционных операторов с полиномиальной сложностью. Это создает предпосылки для арифметизации и распараллеливания логических вычислений.

ПАЛ включает громоздкий аппарат многопараметрических эквивалентных преобразований и сложных позиционных операторов. Плохо формализуемый процесс представления ФАЛ от n переменных в известном методе ПАЛ [2] сводится к построению множества всех операторов порядка n. Из него подбирается оператор, генерирующий наиболее сходную с данной ФАЛ, а затем – последовательность эквивалентных преобразований. При больших n использование такого метода становится крайне трудоемким.

Разработан метод представления ФАЛ на основе позиционных операторов со сложностью не выше 2 и лишь одного вида эквивалентных преобразований, основанный на взаимодействии булевой алгебры логики (БАЛ) и ПАЛ. ФАЛ покрывается задаваемыми своими конъюнкциями $\left(\bigwedge_{t=1}^{n-k} \tilde{x}_{\alpha t} \right)$ фрагментами, каждый из которых записывают посредством простого позиционного оператора и ФАЛ коррекций $f^1_{кор\,i}$ и $f^0_{кор\,i}$:

$$f_i = \left(\bigwedge_{t=1}^{n-k} \tilde{x}_{\alpha t} \right) \wedge \left(f^1_{кор\ i}(X_k) \vee (\boldsymbol{S}^k_{j_i}[X_k] \wedge f^0_{кор\ i}(X_k)) \right),$$

где X_k – входной набор аргументов; $\boldsymbol{S}^k_{j_i}$ – простой позиционный оператор, генерирующий наиболее близкую к f_i ФАЛ-прототип.

Дизъюнкция всех f_i упрощается по правилам БАЛ и ПАЛ. По соотношениям между ними ФАЛ записывается окончательно:

$$z = S^{r}_{2^{r+1}-2}(D_1,...,D_r),$$

где $D_1,...,D_r$ – операторные формы в упрощенной дизъюнкции.

В отличие от известного разработанный метод предполагает для представления ФАЛ не подбор, а формирование позиционных операторов и однопараметрического эквивалентного λ-преобразования, поэтому его трудоемкость многократно меньшая. Метод хорошо формализуем. При этом сохраняется полиномиальная сложность представления ФАЛ.

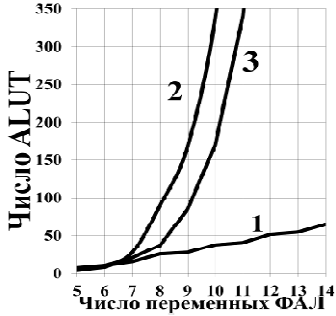

Рис. 1. Ресурсоемкость КС

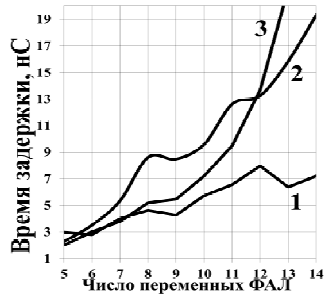

Рис. 2. Быстродействие КС

В соответствии с методом разработана комбинационная схема (КС) для реализации значительного числа ФАЛ. Выполненная на базе ПЛИС при n>7 она обеспечивает существенно меньшие ресурсоемкость (рис. 1) и быстродействие (рис. 2) (зависимость 1), чем КС на основе известных методов реализации ФАЛ (мультиплексора (зависимость 2) и каскадов (зависимость 3)).

Предложен способ распараллеливания логических вычислений и структура исполнительных элементов для его реализации.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Бортовые системы управления космическими аппаратами: учеб. пособ. / Бровкин А.Г. [и др.]; ред. А.С. Сыров. – М.: МАИ-ПРИНТ, 2010. – 304 с.

2. Тельпиз М.И. Принцип позиционности для счисления и исчисления функций / М.И. Тельпиз – М.: ИКИ РАН, 2001. – 457 с.

УДК 044.724.4(045)

А. В. Коган, к.т.н.,
В. В. Храпов, магистр
НТУУ "КПИ" им. И. Сикорского, Киев

МОДЕЛИРОВАНИЕ ТРАФИКА В MESH-СЕТЯХ С ОПРЕДЕЛЕННЫМ КАЧЕСТВОМ ОБСЛУЖИВАНИЯ

В современных условиях развития компьютерных сетей важной и актуальной задачей является переход от разнородных сетей, каждая из которых выполняет узкий спектр услуг, к мультисервисным сетям. Важной частью системы управления такой сетью является надежная система управления трафиком.

Проблема оптимального распределения и качественного управления трафиком изучается продолжительный период времени. Однако и сейчас эта проблема не утратила своей актуальности. Основными задачами на сегодняшний день являются:

– создание четкой теоретической базы при проектировании современных систем распределения информации с учетом мультимедийного трафика;

– создание единой модели пульсирующего трафика;

– разработка методики расчета параметров и показателей качества систем распределения информации с учетом мультимедийного трафика;

– разработка алгоритмов и механизмов качественного обслуживания систем в условиях пульсирующего трафика.

Для эффективного управления трафиком в беспроводных сетях необходимо обеспечить равномерную загрузку сети с учетом требуемого уровня качества обслуживания. При передаче трафика, проходящего по нескольким маршрутам, и дополнительной нагрузке на узлы, задача оптимального распределения трафика с минимальными потерями пакетов данных является особенно актуальной в настоящее время. Для решения этой задачи было предложено:

– правильно распределить входящий трафик;

– минимизировать вероятность потерь пакетов данных;

– увеличить безопасность передачи пакетов данных в сети за счет использования много путевой маршрутизации;

Разработан метод управления трафиком на основе теории игр (как один из вариантов), где выбор маршрута будет происходить исходя из надежности маршрута и вероятности выхода узла из строя.

В разработанном алгоритме управления трафиком основанном на теории игр, в качестве игроков мы будем рассматривать пакеты разнородного трафика, а стратегии – маршруты, по которым происходит доставка пакета от одного абонента к другому. Выиграшем будем считать такую выборку игроком стратегии, которая гарантирует доставку пакета в место назначения с минимальными потерями или без них. Поэтому оптимально выбранная игроком стратегия поможет оптимально загрузить сеть и распределить трафик в ней.

Распределение нагрузки по множеству сформированным путям передачи данных между двумя узлами является также не маловажной задачей. Во многих ситуациях при передачи данных по пути, суммарный передаваемый трафик может в несколько раз превышать максимально допустимую пропускную способность пути. В нашем случае правильным решением есть деление сообщения на части и передача его по нескольким путям.

При высокой скорости движения информации по сети, пакеты поступают на узел не по отдельности, а целиком. Трафик в таких сетях имеет ярко выраженный всплесковый характер, что повышает вероятность перегрузок в узлах сети. Поэтому предотвращение возникновения перегрузок на пути также являются важными задачами и требуют создания запасного безопасного механизма для передачи информации, который гарантирует непрерывность обслуживания в случае сбоя.

Основными мерами предотвращения перегрузок мы предлагаем:

– изменить маршрут передачи данных для обхода проблемного узла.(например, схема живучести);

– перенаправить весь поток на другой менее безопасный путь. В случае перегрузки основного пути, перенаправляем весь трафик на альтернативный менее безопасный маршрут, но безопасность информации также сохраняется;

– распределить трафик с основного пути на все не загруженные пути независимо от уровня их безопасности.

УДК 004.052.42

В. Ю. Куц, к.т.н.,
В. Г. Іванов
Національний технічний університет України КПІ ім. І. Сікорського, Київ

МЕТОД РЕЗЕРВУВАННЯ ТА ВІДНОВЛЕННЯ ДАНИХ В СИСТЕМАХ ЇХ ВІДДАЛЕНОГО ЗБЕРІГАННЯ

Прискорений розвиток засобів телекомунікацій та комп'ютерних мереж стимулює інтенсивний розвиток віддаленого зберігання та обробки даних в рамках хмарних технологій.

Ключового значення набуває проблема забезпечення неперервності доступу користувачів до віддалених даних. Фактично, мова йде про зберігання важливої для користувача інформації на віддалених, не підконтрольних йому носіях, потенційно доступних для стороннього впливу, для яких реально існує ризик втрати даних або тимчасового доступу до них.

Для забезпечення неперервності доступу кожному користувачеві до своєї інформації використовується резервування.

Найбільш простою схемою резервування є просте дублювання даних. До такого типу відносяться системи Intermemory та RAID-1. 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. Найбільш відомим застосуванням такої схеми резервування є система RAID-2. Проте вона не дозволяє відновлювати дані при втраті доступу до більш як одного носія.

Авторами пропонується підхід до рекурсивного відновлення з довільної непарної кількості p носіїв, до яких втрачено доступ, на основі представлення інформації користувача у вигляді матриці M, рядки якої співвідносяться з носіями, а стовпці - з фрагментами, на які розбиваються дані. В якості резервних пропонується використати: один носій, кожен фрагмент зберігає суми за модулем 2 однойменних стовпців матриці M; $(p-1)/2$ носіїв, кожен фрагмент яких зберігає суми за модулем 2 фрагментів, розташованих на

низхідних діагоналей матриці М, з кутом нахилу -45°, -22°,…,-90°/ (*p*-1); (*p*-1)/2 носіїв, кожен фрагмент яких зберігає суми за модулем 2 висхідних діагоналей з кутом нахилу 45°, 22°,…,90°/ (*p*-1).

Відновлення даних з *p* віддалених носіїв, до яких втрачено доступ пропонується виконувати за наступною схемою.

1) Номер *j* фрагменту встановити в одиницю: *j*=1;.

2) поточний кут α висхідної діагоналі матриці М встановлюється рівним 90°/ (*p*-1): .α = 90°/ (*p*-1); поточний кут β низхідної діагоналі встановлюється рівним -90°/(*p*-1): β = -90°/ (*p*-1);

3) в *j*-тому стовпці матриці М знаходиться фрагмент ξ, доступ до якого втрачено, з найменшим номером рядка. Знайдений фрагмент ξ відновлюється з використанням резервної суми фрагментів, що лежать в матриці М на висхідній діагоналі під кутом α, якій належить і фрагмент ξ. Значення α подвоюється: $\alpha=2\cdot\alpha$;

4) в *j*-тому стовпці матриці М знаходиться фрагмент η, доступ до якого втрачено, з найбільшим номером рядка. Знайдений фрагмент η відновлюється з використанням резервної суми фрагментів, що лежать в матриці М на низхідній діагоналі під кутом β, якій належить і фрагмент η. Значення β подвоюється: $\beta=2\cdot\beta$;

5) якщо $\alpha<90°$, здійснюється повернення на повторне виконання п.3, інакше з використанням резервної суми *j*-того стовпці відновлюється останній фрагмент цього стовпця;

5) здійснюється перехід на наступний фрагмент: *j*=*j*+1, якщо *j*<=*n*, то виконується перехід на п.2, інакше кінець.

Основною відмінністю запропонованого методу є те, що він не накладає обмежень на кількість носіїв, дані з яких можуть бути відновлені. Оскільки для відновлення даних з *p* носіїв використано таку ж кількість резервних носіїв, то метод забезпечує теоретичний мінімум інформаційної надлишковості резервування даних.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Марковський О.П. Організація резервування та відновлення даних при їх віддаленому зберіганні / Марковський О.П., Іванов Д.Г., Ванчугов Б.Ю. // Вісник Національного технічного університету України ”КПІ” Інформатика, управління та обчислювальна техніка, – Київ: ВЕК+ – 2013. – № 59. − С. 50-55.

УДК 004.042.52

О. П. Марковський, к.т.н.,
Лефтеріос Захаріудакіс, аспірант,
М. Ф. Федотов
Національний технічний університет України
КПІ ім. І.Сікорського, Київ

МЕТОД ШВИДКОЇ СТРОГОЇ ІДЕНТИФІКАЦІЇ ВІДДАЛЕНИХ КОРИСТУВАЧІВ

Розвиток хмарних технологій дозволяє надати широкому колу користувачів доступ значного обсягу інформаційних, обчислювальних та програмних ресурсів. Разом з тим, розвиток хмарних технологій породжує ряд проблем, пов'язаних з захистом даних та розподіленням прав доступу до них. В світлі цього, ключового значення набуває проблема ідентифікації віддалених користувачів.

Комерціалізація віддаленого надання ресурсів вимагає суттєвого підвищення надійності ідентифікації. З іншого боку, збільшення кількості користувачів диктує необхідність підвищення швидкості ідентифікації. Вказані чинники зумовлюють актуальність розробки нових методів ідентифікації.

Теоретично доведено [1]., що найбільша протидія незаконному доступу до віддалених ресурсів досягається при виконанні умов:

- пароль має змінюватися в кожному сеансі ідентифікації і генеруватися спеціальним механізмом;

- система має механізм перевірки паролю, але не може сама генерувати пароль.

Ідентифікація, що відповідає вказаним вимогам називається строгою або такою, що відповідає концепції "нульових знань" [1].

До теперішнього часу розроблено ряд криптографічних механізмів, що реалізують строгу ідентифікацію. Найбільш відомимі з них FFSIS, методи Шнора та Гіллоу-Квіскватера [1]. В якості математичної основи всіх цих криптографічних механізмів використовуються мультиплікативні операції модулярної арифметики, що виконуються над числами, розрядність яких становить нині 2048-4096 і значно перевищує розрядність процесора. Відповідно, ці реалізація цих механізмів строгої ідентифікації потребує значних за обсягом обчислювальних ресурсів.

Авторами запропоновано метод реалізації строгої ідентифікації

на іншій математичній основі - незворотних булевих функціях. Для реалізації таких перетворень пропонується використати стандартизовані хеш-перетворення SHA-1, Ripemd-160 [1].

Метод передбачає таку послідовність дій при реєстрації :

1) Користувач довільно визначає кількість n циклів ідентифікації.

2) Випадковим чином генерує n–тий сеансовий пароль P_n.

3) Обчислює n-1 паролів, причому j-тий пароль P_j, j=n-1,…,0 обчислюється як хеш-перетворення H(x) від конкатенації попереднього паролю та номера сеансу: $P_j = H(P_{j+1} \| j)$.

4) Пароль P_0 відсилається в систему, зашифрований її відкритим ключем.

Послідовність дій j–того сеансу ідентифікації має вигляд:

1) Користувач шифрує відкритим ключем системи j-тий сеансовий пароль P_j і відсилає його в систему.

2) Система виконує хеш-перетворення над конкатенацією отриманого паролю та номера сеансу: $\xi = H(P_j \| j)$ і порівнює результату з попереднім паролем P_{j-1} : якщо $\xi = P_{j-1}$ то надається доступ.

Очевидно, що система, маючи в розпорядженні попередній пароль P_{j-1} не здатна сама генерувати наступний пароль P_j : ця задача еквівалентна злому стандартизованого хеш-алгоритму. Ці алгоритми ретельно тестовано,вони пройшли апробацію практикою, їх незворотність гарантована відповідними державними органами. Виходячи з цього, можна вважати, що задача підбору пароля як системою так і стороннім зловмисником потребує ресурсів, що виходять за рамки практичної доцільності.

Основною перевагою запропонованого метода в порівнянні з аналогами полягає в тому, що передбачені ним обчислення мають значно меншу складність. За оцінками [1] швидкість реалізації стандартизованих хеш-перетворень SHA-1 та Ripemd-160 на три порядки більша ніж виконання модулярного експоненціювання.

Проведені експерименти показали, що реально швидкість ідентифікації збільшується на 2-3 порядки.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Schneier B. Applied Cryptography. Protocols. Algorithms and Source codes in C. − Ed.John Wiley, 1996 − 758 p.

УДК 004.056.5

О. П. Марковський, к.т.н.,
К. О. Шапран
Національний технічний університет України «КПІ ім. І. Сікорського», Київ

МЕТОД КОРЕКЦІЇ ОДНОКРАТНИХ ПОМИЛОК СИНХРОНІЗАЦІЇ В ПОСЛІДОВНИХ КАНАЛАХ ПЕРЕДАЧІ ДАНИХ

Динамічний розвиток комп'ютерних систем супроводжується стрімким прогресом засобів передачі даних між їх компонентами. У той же час склалася тенденція до збільшення швидкості передачі даних, в основному за рахунок зменшення надійності. Зростання швидкості передачі неминуче впливає на збільшення кількості помилок. Відомі методи не забезпечують ефективного вирішення задачі знаходження і корекції великої кількості помилок синхронізації [1]. Тому, метою дослідження є розробка методу ефективної корекції всіх помилок синхронізації в темпі передачі цифрових даних між компонентами комп'ютерних систем з використанням послідовних каналів.

Для досягнення поставленої мети пропонується метод корекції всіх однократних помилок синхронізації. Розроблений метод передбачає наступну модель виникнення помилок синхронізації при передачі n-бітового блоку B_S даних у послідовному каналі. Виникнення помилки синхронізації можливе тільки у фрагментах, які є послідовність одиничних біт, кількість яких більша або дорівнює критичній межі $h = 6$ (для USB порту). Тому, в блоці B_S, що передається, виділяються всі послідовності одиниць, довжиною не меншою за $h - 1$: E_{1S}, E_{2S}, …, E_{mS}, де m – кількість фрагментів у блоці. Довжини цих фрагментів: l_{1S}, l_{2S}, …, l_{mS}, $\forall i = 1, \ldots, m$; $l_{iS} \geq h - 1$. На стороні передавача пропонується обчислити контрольну послідовність S, яка складається з двухбітних символів $c_{1S}, c_{2S}, \ldots, c_{mS}$, де $c_{iS} \in \{0,1,2,3\}$, $i \in \{1,..,m\}$, кожний з яких обраховується за формулою: $c_{iS} = l_{iS} \bmod 4$. Контрольна послідовність S передається разом з інформаційним блоком B_S. Прийнятий блок даних B_R, аналізується аналогічним чином до відправленого: виділяються фрагменти E_{1R}, E_{2R}, .. E_{mR}, що мають довжини: $l_{1R}, l_{2R}, \ldots, l_{mR}$, $\forall i = 1, \ldots, m$; $l_{iR} \geq h - 1$. На стороні приймача,

використовуючи блок B_R, пропонується обчислити контрольну послідовність R двухбітних символів $R = \{c_{1R},c_{2R},\ldots,c_{mR}\}$, де $c_{iR} = l_{iR} \bmod 4$.

Рішення задачі виявлення помилок синхронізації пропонується здійснювати шляхом порівняння та аналізу двох контрольних послідовностей: отриманої від передавача та обрахованої на приймачі. Якщо всі відповідні символи контрольних послідовностей рівні між собою: $\forall i \in \{1,2,..,m\}$: $c_{iS} = c_{iR}$, то блок переданий без помилок. В іншому випадку, при $c_{iS} \neq c_{iR}$, у блоці виникла помилка синхронізації при передачі i-того фрагмента. Для виявлення типу помилки, пропонується перевірити гіпотезу про те, що довжина i-го фрагмента було помилково збільшена на одиницю на стороні приймача. Для цього обраховується $(c_{iS}+1) \bmod 4$ та порівнюється з відповідним символом контрольної послідовності приймача c_{iR}. При виконанні умови $(c_{iS}+1) \bmod 4 = c_{iR}$ вказана вище гіпотеза справедлива, тому приймається рішення про корекцію i-го фрагмента шляхом вилучення з нього одиниці. Якщо $(c_{iS}+1) \bmod 4 \neq c_{iR}$ приймається рішення про наявність помилки синхронізації, а саме зменшення на стороні приймача кількості одиниць в i-тому фрагменті: для корекції такої помилки виконується додання одиниці до i-того фрагмента прийнятого блоку.

У результаті проведених досліджень запропоновано метод корекції всіх однократних помилок синхронізації. Основна перевага методу, у порівнянні з існуючими, це відсутність обмежень на кількість помилок, що можуть бути виправлені. Іншою важливою перевагою методу є використання простих операцій, що забезпечує високу ефективність апаратної реалізації. Запропонований метод орієнтовано для швидкісних послідовних каналів обміну цифровими даними між компонентами комп'ютерних систем.

ВИКОРИСТАНІ ДЖЕРЕЛА

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

УДК 004.(043.2)

О. О. Мелешко,
Д. Р. Коваль
Національний авіаційний університет, Київ

ТЕХНОЛОГІЇ ПРИСКОРЕНОЇ РОЗРОБКИ FRONT-END

Розробка front-end виключно засобами HTML, CSS та JS є досить рутинним заняттям. Через це було розроблено велику кількість засобів для поліпшення front-end розробки. Найбільш розповсюдженими засобами є такі засоби як менеджери пакетів, засоби для автоматизації процесів front-end розробки, CSS-препроцесори та HTML-препроцесори, CSS-постпроцесори.

Менеджери пакетів. Одним з рутинних занять є завантаження в проект сторонніх бібліотек, таких як JQuery, Bootstrap, Fotorama, Owl Carousel, та інші а також інших програмних засобів призначених для поліпшення розробки. Для їх завантаження необхідно виконувати завантаження архівів, їх розпакування, копіювання, встановлення завантажених програм. Менеджери проектів спрощують цей процес замінюючи його на декілька команд в терміналі. Найбільш популярними менеджерами пакетів на сьогоднішній день є Node.js Package Manager(NPM) та Bower. Дані менеджери пакетів за рахунок своєї специфікації, за часту використовуються разом. NPM був розроблений для серверного JS на відміну від Bower, котрий був розроблений для клієнтського JS. Оосновною відмінністю даних менеджерів пакетів є те, що NPM встановлює кожен пакет з окремою для нього залежністю, у результаті утворюється велике дерево пакетів у котрому може знаходитись одразу декілька версій одного пакету. На клієнтській частині JS це не є допустимим, тому Bower кожен пакет встановлюється один раз а у випадку конфлікту, відмовить у повторному встановленні вже існуючого пакету. Також дані менеджери пакетів підтримують встановлення пакетів по файлам bower.json для Bower та package.json для NPM, в котрих міститься перелік назв та версій пакетів, що спрощує перенесення пакетів між проектами.

Автоматизація процесів. У ході front-end розробки, є безліч процесів, котрі потрібно повторювати раз за разом, таких як формування спрайтів з SVG та PNG, стиснення зображень до

допустимого порогу, компіляція препроцесорів, об'єднання файлів проекту у один та його мінімізація, тощо. Grunt та Gulp – найбільш розповсюджені інструменти для автоматизації таких процесів. Дані інструменти є конкурентами. Grunt виник в кінці 2011 року і на сьогоднішній день містить близько 4700 додатків. Gulp є більш новим а саме, вийшов у середині 2013 року і нараховує близько 1700 додатків. На основі додатків, формується функціонал даних інструментів, котрий записується в файли котрі обробляються ними. Gulp є більш швидшим у своїй роботі, що приваблює все більшу аудиторію.

HTML-препроцесори. Метою використання HTML-препроцесорів є поліпшення написання розмітки. Такими препроцесорами є Jade, Slim та Haml (HTML abstraction markup language).

CSS-препроцесори. CSS-препроцесор це інструмент поверх CSS, котрий розширює функціонал CSS, розширює синтаксичні можливості та спрощує синтаксичні конструкції. На даний момент існує три найбільш популярних препроцесора: Less, Sass(SCSS), Stylus.

Sass – найпотужніший і найстаріший з CSS-препроцесорів і був розроблений як модуль для HAML. Має більші можливості ніж Less та можливість їх розширення за рахунок бібліотеки Compass. Має дві синтаксичні конструкції: Sass(Syntactically Awesome Style Sheets) та SCSS(Sassy CSS).

Stylus – наймолодший, але найперспективніший CSS-препроцесор, заснований в 2010 році. Підтримує безліч варіантів синтаксису.

CSS-постпроцесори. На відміну від препроцесорів котрі використовують деяку мову котра компілюється в CSS, постпроцесор на вході отримує вже готовий CSS котрий обробляється парсером та після, додатками котрі модифікують CSS у більш оптимальний та адаптивний вид. Найбільш розповсюдженим інструментом для постпроцесора – PostCSS, котрий також використовується, як препроцесор.

УДК 004.658(043.2)

Л. О. Ничипоренко,
Національний Університет Біоресурсів і Природокористування України, Київ
В. О. Рудюк
Національний Університет Харчових Технологій, Київ

СИСТЕМА ПРОДАЖУ ТА УПРАВЛІННЯ ТОВАРОМ

Одним з ефективних напрямків удосконалення управління підприємством є розробка та впровадження сучасних інформаційно-управляючих систем і технологій. Нові інформаційні технології управління підприємством є важливим і необхідним засобом, який дозволяє:

- швидко, якісно і надійно виконувати отримання, облік, зберігання і обробку

інформації;

- значно скоротити управлінський персонал підприємства, який займається роботою по збору, обліку, зберіганню і обробці інформації;

- забезпечити у потрібні терміни керівництво і управлінсько-технічний персонал підприємства якісною інформацією;

- своєчасно і якісно вести аналіз і прогнозування господарської діяльності підприємства;

-швидко і якісно приймати рішення по усіх питаннях управління підприємством.

Для правильного керівництва діяльністю торгового підприємства необхідно мати повну, точну, об'єктивну, своєчасну та досить детальну економічну інформацію. Це досягається веденням сучасного бухгалтерського та логістичного обліку на підприємстві.

Початковим етапом бухгалтерського обліку є суцільне документування всіх господарських операцій шляхом складання певних матеріальних носіїв первинної облікової інформації.

Для документування операцій можуть застосовуватися типові міжвідомчі форми, а також форми, самостійно розроблені стосовно до відповідних типовим, що містить обов'язкові реквізити та забезпечують достовірність відображення в обліку зроблених операціях.

До обов'язкових реквізитів первинних облікових документів належать:

• найменування документа (форма);

• дата складання;

• зміст господарської операції;

• вимірювачі господарської операції (у кількісному і вартісному вираженні);

• найменування посадових осіб, відповідальних за здійснення господарської операції і правильність її оформлення;

• особисті підписи та їх тлумачення.

Порядок і строки як прийому, так і реалізації товарів за кількістю, якістю та комплектності та його документального оформлення обумовлені діючими технічними умовами поставки, договорами купівлі-продажу та інструкціями про порядок приймання товарів за кількістю, якістю та комплектності.

Облік реалізації товарів неможливо правильно організувати без належного обліку товарів у місцях їх зберігання. Облік товару на складі оптового підприємства веде матеріально відповідальна особа. Складський облік ведеться в натуральних показниках за номенклатурними номерами товарів (тари) на підставі відповідних прибуткових і видаткових документів. Порядок обліку товару на оптовому складі може бути різний залежно від способу зберігання товару і від різних факторів. У будь-якому випадку товари, що зберігаються на складі, повинні бути забезпечені товарним ярликом. Найзручніше, коли метод зберігання збігається з аналітикою в бухгалтерському обліку.

В організації торгівлі реалізація товарів оформляється товаро-супровідними документами, передбаченими умовами поставки товарів і правилами перевезення вантажів (накладної, товарно-транспортної накладної, залізничної накладної).

Матеріально відповідальні особи складів на підставі прибуткових і видаткових документів роблять записи в картках складського обліку, складають товарні звіти та супровідні реєстри здачі документів. Форма звітності залежить від спеціалізації оптового підприємства, асортименту товарів, обсягу документообігу та організації аналітичного обліку товарів у бухгалтерії та способу зберігання. Після цього первинні документи разом з відповідними реєстрами і звітами здаються в бухгалтерію.

УДК 004.716

Р. С. Одарченко, к.т.н.,
Д. Д. Вергелес,
А. О. Абакумова, асп.,
Н. В. Дика
Національний авіаційний університет, Київ

ВИЗНАЧЕННЯ ПЕРСПЕКТИВНИХ ВАРІАНТІВ ПОБУДОВИ ТРОПОСФЕРНИХ ЛІНІЙ ЗВ'ЯЗКУ

Однією із ключових особливостей тропосферного розповсюдження радіохвиль є суттєвий вплив погодних факторів, які проявляються у короткотермінових та довготермінових затуханнях і обумовлюються, в основному, наявністю водяної пари в атмосфері [1].

Таким чином, при проектуванні тропосферних телекомунікаційних станцій доцільно передбачати регулювання потужності випромінювання у залежності від стану атмосфери. Окрім енергетичного виграшу, це також сприяє підвищенню скритності тропосферної системи зв'язку. Тому забезпечення постійного моніторингу умов розповсюдження радіохвиль з відповідним регулюванням потужності випромінювання є одним із важливих принципів конструювання ТРС. Разом з тим, можна допустити, що для спеціального використання, при побудові ТРС з порівняно невеликими швидкостями передавання інформації, можна досягнути певних переваг застосовуючи активні методи. Зокрема, шляхом використання шумоподібних (ШПС), псевдошумових сигналів (в яких добуток ширини спектру на його протяжність, база >> 1) у сполученні зі згортковим кодуванням інформації за алгоритмом Вітербі. У такій системі досягається ефект неявного частотного та часового рознесення. Неявне частотне рознесення забезпечується за рахунок передавання цифрової інформації з шириною спектру більшою, ніж смуга кореляції каналу зв'язку та шляхом надлишкового кодування з перемежуванням для декореляції похибок [2].

Таким чином, передбачається, що використання ШПС у перспективній ТРС дасть можливість досягти ряд важливих переваг:

– висока вірогідність приймання сигналів при потужності

перешкод у смузі частот набагато більшій, ніж потужність сигналу, що обумовлює підвищення;

– завадостійкості в умовах дії штучно створених, навмисних перешкод;

– висока роздільна здатність сигналів і, як наслідок цього, можливість ефективної роботи ТРС в умовах багатопроменевого поширення радіохвиль і міжсимвольної інтерференції;

– можливість передавання інформації у завантаженому каналі зв'язку без суттєво помітних впливів на роботу інших засобів зв'язку;

– можливість побудови асинхронних багатоадресних систем з ретрансляторами і кодовою адресацією.

Аналіз технічних особливостей наявних на ринку інформаційних послуг ТРС свідчить, що їм притаманні суттєво більші потужності випромінювання (від 0,1 до 3 кВт), ніж у звичайних релейних станціях прямої видимості. Технічні засоби для реалізації таких потужностей випромінювання – мають доволі складну конструкцію і, відповідно, невисоку надійність (питання ціни не розглядаємо, бо воно для ТРС спеціального призначення має другорядне значення).

Враховуючи це, перспективним видається технічне рішення щодо виконання антени у вигляді активної приймально-передавальної антенної решітки. Якщо, при цьому, приймач також побудувати з розділеним підсиленням, а в кожній приймально-передавальній комірці до передавального та приймального трактів ввести регульовані фазообертачі та атенюатори, можна отримати додаткову функцію електронного регулювання положення діаграми спрямованості антени (на приймання та передавання незалежно). При цьому, вихід із ладу декількох комірок, загалом, може вплинути на загальну роботоспроможність ТРС, але повністю з ладу її не виведе, що в умовах кризових ситуацій є суттєвою перевагою.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Давыденко Ю.И. Дальняя тропосферная связь. – М. Воениздат, 1968.

2. Серов В.В. Помехоустойчивость пространственно частотных кодовых конструкций в каналах с релеевскими замираниями. // Радиотехника, №12,1994.

УДК 004:656.614.2

Л. М. Олещенко, к.т.н.,
Д. П. Ландяк,
В. В. Миколайчик
НТУУ «КПІ ім. І.Сікорського», Київ

ОН-ЛАЙН СИСТЕМА ДИСПЕТЧЕРСЬКОГО УПРАВЛІННЯ АВТОБУСНИМИ ПАСАЖИРСЬКИМИ ПЕРЕВЕЗЕННЯМИ

У зв'язку з нераціональним використанням транспортних засобів (ТЗ) для міжміських пасажирських перевезень, не ефективно створеними розкладами перевезень, або ж їх відсутності та поганою організацією роботи персоналу, виникає необхідність у створенні ефективного програмного продукту, який дозволятиме вводити інформацію про навантаженість пасажиропотоку у режимі он-лайн. Використовуючи ефективне програмне забезпечення, диспетчер зможе збирати дані про кількість пасажирів, яким потрібно було дістатися з одного пункту в інший. Після отримання інформації має проводитися її аналіз для оптимізації роботи рухомого складу автотранспортного підприємства (АТП) та виконання прогнозу пасажиропотоку на конкретну годину, день чи тиждень з урахуванням вихідних, свят та циклічності пасажиропотоку.

В Україні організація пасажирських автобусних перевезень в основному відбувається на основі складання розкладу руху автобусів. Розклад є в пункті відбуття і призначення. Автобуси виїжджають чітко за розкладом, вони можуть виходити у рейс інколи напівпорожніми. Такі явища є збитковими для АТП. Через нестабільність потоку людей дуже тяжко реалізувати адекватний розклад, щоб задовольнити користувачів та автостанції. В Європі прогресивно використовується моделювання в реальному часі. Наприклад, німецька компанія "bahn.de"[1] формує рух автобусів за кількістю приїхавших людей до міста потягами та літаками. Це зменшує черги, заповненість автобусів стає оптимальною. В США працює уже близько 20 років компанія FDOT [2], що аналізує весь автопотік на шосе та дорогах, по зібраній інформації формується швидкісний режим, темп світлофорів та регулювання потоку для створення мінімальних заторів та відсутності аварій.

Розроблюване програмне забезпечення для вирішення даної проблеми повинне працювати в мережі Інтернет, бути надійним, ефективним та зручним у користуванні. При розробці продукту необхідно дотримуватися наступних вимог:

- мультиплатформенність та ефективність продукту;
- сучасність;
- простота використання, низький поріг входження.

Враховуючи складність системи, було прийняте рішення про її розбиття на компоненти:

- серверна частина;
- клієнтська частина для веб-браузерів;
- клієнтська частина для смартфонів на базі ОС Android.

Для взаємодії даних компонентів використано REST - підхід до архітектури мережевих протоколів, які забезпечують доступ до інформаційних ресурсів. Серверна частина продукту розроблена з використанням засобів мови програмування Java та фреймворку Spring. Клієнтська частина продукту для веб-браузерів реалізована з використанням HTML5 та CSS3. Клієнтська частина для смартфонів розроблена за допомогою мови програмування JavaScript та фреймворку React Native. Програмні модулі розроблюваної он-лайн системи забезпечують виконання прогнозу пасажиропотоку з використанням гармонічного аналізу Фур'є та модифікованої гравітаційної моделі пасажирсько-транспортної взаємодії між містами. Розрахунок необхідного рухомого складу АТП здійснюється методом нелінійного математичного програмування, де в якості цільової функції виступають сумарні витрати по забезпеченню пасажирських перевезень на маршруті, в якості обмежень – кількість одиниць транспорту різного типу тощо [3]. В даній системі диспетчер отримує оптимальні рішення по структурі рухомого складу, враховується собівартість ТЗ, є можливість виключати з аналізу транспорт, що вийшов з ладу.

ВИКОРИСТАНІ ДЖЕРЕЛА

1.DB Vertrieb GmbH // https://www.bahn.com

2.Florida Department of Transportation // http://www.fdot.gov

3. Medvedev M.G., Oleshchenko L.M. The optimal control models of interurban bus transport // Electronics and control systems. – 2014.– №1(39). – P. 85-90.

УДК 004.274

В. М. Опанасенко[1], д.т.н.
Э. Э. Эсанов[2], к.т.н.
[1] *Институт кибернетики НАН Украины, Киев*
[2] *ТГТУ, Ташкент*

СТРУКТУРНАЯ ОРГАНИЗАЦИЯ УСТРОЙСТВ СОРТИРОВКИ НА БАЗЕ FPGA

Решение широкого круга задач требует использования операций сортировки заданного массива данных. В качестве меры эффективности реализации алгоритма сортировки обычно принимают число необходимых сравнений и число пересылок (перестановок) элементов. В общем случае, эти значения определяют функцию от N – числа сортируемых элементов, т.е. глубину массива. Прямые методы сортировки требуют порядка N^2 сравнений элементов, а ускоренные методы – до $(\log_2 N)$ сравнений [1].

Рассмотрим FPGA–реализацию операции сортировки – линейный сортировщик [2], который позволяет совмещать время ввода–вывода данных со временем сортировки.

Сортировщик выполняет отображение $\Lambda(X \Rightarrow Y)$ таким образом, что на его вход последовательно поступает множество $X = \{x_\omega : \omega = 1 \div N\}$, а на выходе последовательно формируется множество $Y = \{y_\alpha : \alpha = 1 \div N\}$ ($Y = X$, $y_\alpha \le y_{\alpha+1}$).

Линейный сортировщик обрабатывает множество элементов X ($Card\{X\} = N$) и включает $N/2$ функциональных блоков, каждый из которых состоит из двух регистров (P_i и Q_i, $i = 1 \div (N/2)$) и компаратора. В исходном состоянии регистры P_i и Q_i содержат максимальное значение данных. На входном этапе n элементов сортируемого массива последовательно поступают в регистр Q посредством сигнала сдвига вправо. После сдвига выполняется сравнение содержимого регистров P_i и Q_i, при этом меньшее значение перемещается в регистр P_i. На выходном этапе регистры P_i выполняется сдвиг влево за N циклов и в освобождающиеся регистры загружается максимальное значение – единичный вектор.

В случае равенства нескольких элементов за min принимается элемент, который первым поступил на вход сортировщика.
Блок–схема алгоритма сортировки приведена на рис.1.

Обрабатывающие блоки реализованы посредством схемного редактора с помощью CORE генератора, а устройство управления – State Editor системы проектирования ISE Foundation на основе кристаллов FPGA серии Virtex–6. Аппаратные и временные оценки для 16–разрядных данных (ширина массива) для $N = 8, 16$ (глубина массива) приведены в табл.1.

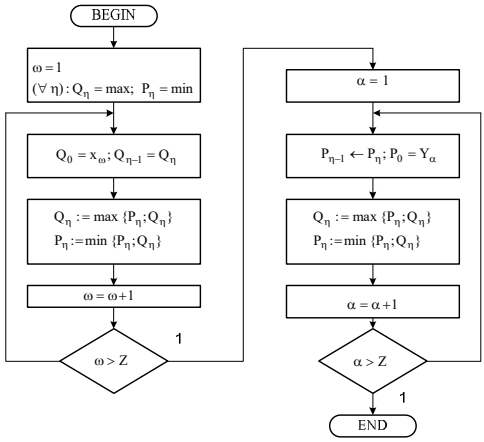

Рис.1. Блок–схема алгоритма сортировки

Таблица 1.

Аппаратные и временные оценки линейного сортировщика

Размерность массива сортировки (глубина×ширина)	16×16	8×16
Количество слайсов (Slices)	596	313
Период (нс) /частота тактирующих сигналов (МГц)	10,5/95	9/111
Время сортировки массива, нс	1008	432

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Кнут Д. Искусство программирования для ЭВМ, т.3.: Пер. с англ. – М.: Мир, 1978. – 723с.

2. Choi Y.–H. Easily reconfigurable VLSI sorter // Int. Journal Electronics. – 1990. – Vol.69, N.3. – P. 369 –378.

УДК 004.056.53

П. В. Пасічник,
Б. Я. Корнієнко, д.т.н.
Національний авіаційний університет, Київ

ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ FTP-СЕРВЕРА

Хоча приєднання до Інтернету надає величезні вигоди у вигляді доступу до колосального обсягу інформації, воно не обов'язково є хорошим рішенням для організацій з низьким рівнем безпеки. Інтернет страждає від серйозних проблем з безпекою, які, якщо їх ігнорувати, можуть призвести до жахливих наслідків для непідготовлених мереж. Помилки при проектуванні сервісів TCP / IP, складність конфігурації хостів, вразливі місця, що з'явилися в ході написання програм, і ряд інших причин в сукупності роблять непідготовлені мережі відкритими для діяльності зловмисників і вразливими до пов'язаними з цим проблем.

Для підвищення захищеності на сервері FTP можна впровадити один або кілька варіантів модулів аутентифікації з другим фактором і прив'язати до них користувачів.

У більшості випадків, PAM можна вказати і в конфігурації FTP серверів, і принципі проблема безпеки FTP буде вирішена таким же чином. Але в залежності від швидкості з'єднання, налаштувань сервера або режиму FTP з'єднання FTP сесія може перериватися при відсутності активності протягом певного часу. У «класичному» FTP клієнт просто підключиться ще раз, треба просто поставити галочку «зберегти пароль». У разі ж двох факторної аутентифікації це не спрацює, доведеться вводити пароль і код з «токена» досить часто, що незручно для користувача.

Для вирішення проблеми можна зробити парольний додаток з активованою двоетапної аутентифікації. Для цього потрібно розробити веб-інтерфейс для генерації парольних додатків. Сам веб-інтерфейс буде доступний тільки з використанням двоетапної аутентифікації. Після входу в систему, користувач буде генерувати FTP пароль, який буде активний тільки протягом певного часу і тільки для певного IP адреси (рис.1).

При генерації скрипт заносить дані в таблицю бази даних, а саме ім'я користувача, IP адресу і часову мітку зазначеного користувачем часу, а також згенерований FTP пароль, який і

показується користувачеві в інтерфейсі. Для доступу по FTP буде використовуватися саме цей тимчасовий пароль(рис. 2).

Рис.1 Приклад графічного інтерфейса

Таблиця temp_passwords

id	username	client_ip	expires	temp_password
1002	ehuseynov	193.168.0.51	1386339927	sZ284X57b3e7v52

Рис.2 Приклад бази даних

Таким чином можливо отримати хост з підвищеною захищеністю каналу передачі даних.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. В.Г. Олифер, Н.А. Олифер - Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. — СПб.: Питер,2010.—944с.:ил.

2. Корнієнко Б.Я. Система інформаційної безпеки / Д.П. Галата, Б.Я. Корнієнко, Л.П. Галата // Збірник наукових праць Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова. – 2011. - Випуск 59. - С. 48 - 52.

3. Корнієнко Б.Я. Прикладні програми управління інформаційними ризиками / Б.Я. Корнієнко, Н.М. Марутовська, Ю.О. Максімов / Захист інформації. – 2012, № 4 (57). - С. 60 - 64.

4. Корнієнко Б.Я. Оцінка ризиків автоматизованої інформаційної системи / Б.Я. Корнієнко, О.К. Юдін, Г.В. Наконечна // Наукоємні технології. – 2012. - № 2 (14). - С. 69-73.

УДК 004.4:001.102:006.35(100)ISO(043.2)

Н. В. Пащенко,
В. М. Мокійчук, к.т.н.
Національний авіаційний університет, Київ

ІНФОРМАЦІЙНА СИСТЕМА УПРАВЛІННЯ ПРОЦЕСАМИ ЛАБОРАТОРІЇ

Відповідно до стандарту ДСТУ ISO\IEC 17025:2006 [1] до випробувальних лабораторій і діючих в них системах управління якістю (СУЯ) пред'являються високі вимоги, що вимагає від лабораторій значних ресурсів. Документообіг СУЯ в акредитованих лабораторіях значно зростає. Постає необхідність використання інформаційних технологій у лабораторній практиці, створення та впровадження інформаційної системи управління процесами лабораторії.

Більша частина внутрішньолабораторного документообігу під час обробки замовлення виконується в паперовому вигляді – у вигляді бланків-заявок на виконання випробувань, лабораторних журналів для обліку результатів досліджень, протоколів випробувань та ін. Такий підхід хоч і є традиційним, але може бути досить незручним і призвести до порушення діяльності лабораторії в цілому.

Обчислення результатів випробувань та супутніх характеристик (наприклад, невизначеності вимірювань або інших параметрів контролю якості) відбувається або вручну, або із застосуванням різних програмних продуктів, які дуже часто не мають можливості взаємодіяти один з одним та автоматично враховувати отримані результати в протоколах випробувань.

Використання інформаційної системи управління процесами лабораторії дозволяє автоматизувати процес прийому замовлень, складання завдання на проведення випробувань, розрахунок результатів вимірювань, невизначеностей та інших значень, формування протоколів випробувань, а також ряду фінансових документів, необхідних для виконання замовлення.

Щоб відповідати вимогам до управління та технічним вимогам стандарту [1], інформаційна система управління процесами лабораторії має мітити наступні функціональні елементи: модуль

обліку зразків і результатів (вибір завдання на випробування, розрахунок необхідних параметрів та реєстрація результатів випробування, розрахунок невизначеності); модуль управління процесом вимірювання (реєстрація умов навколишнього середовища, контроль стану зразка, засобів вимірювальної техніки, якості вимірювання); модуль загального управління лабораторією (контроль правильності введених результатів, сформованих завдань та протоколів випробувань, формування звітності по роботі лабораторії); модуль нормативної документації (створення та підтримка переліку об'єктів випробувань та переліку контрольованих показників, бібліотеки стандартів), модуль управління персоналом (планування та облік навчання, облік атестації, допуск до проведення випробувань).

Одна з основних вимог стандарту [1], якій має відповідати лабораторія та інформаційна система управління процесами в ній, це забезпечення захисту конфіденційності інформації та прав власності її замовників, зокрема процедури зберігання та передавання результатів.

На сьогодні в Україні існують декілька інформаційних лабораторних систем, такі як АСУ «Лабораторія», LeoLAB, «Браво-Лабораторія». Усі вони лише частково задовольняють вимогам стандарту [1]. Крім того, жодна із наявних систем не відповідає вимогам стандарту [2]. Тому створення та використання в лабораторній практиці інформаційної системи управління процесами лабораторії, яка б повністю задовольняла вимогам стандартів [1,2], є актуальними питаннями.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Загальні вимоги до компетентності випробувальних та калібрувальних лабораторій (ISO/IEC 17025:2005, IDT): ДСТУ ISO/IEC 17025:2006. – [чинний від 01.07.2007]. – К.:Держспоживстандарт України, 2007. – 27 с. – (Національний стандарт України).

2. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT): ДСТУ ISO/IEC 27001:2015. – чинний від 01.01.2017]. – К.:Держспоживстандарт України, 2017. – 27 с. – (Національний стандарт України).

UDC 004.93 (043.2)

S. O. Petrenko,
S. O. Kudrenko
National Aviation University, Kyiv

METHOD OF DETECTION MOVING OBJECTS WITH DYNAMIC LIGHTING IN CCTV

Many video surveillance systems set themselves the task to track moving objects in a video in real time. This increases the amount of possible tasks that can execute the system. For example, performing the count of people who entered / left the room can evaluate the effectiveness of shops in different periods of the day, week, month, and year. There will appear an opportunity to determine whether successful store locations, evaluate the effectiveness of marketing activities and advertising campaigns.

It is not difficult to do it in the rooms with artificial lighting. There the sun does not influence the lighting and video stream easier to analyze. However, the problem is video surveillance outdoors or in areas with a large number of windows.

Normal detection of moving objects, which may be people who enter or leave the premises, can be done by the following algorithm:

1. Take a picture in which there are no objects to be tracked. This will be our background;
2. Converts our RGB background in black and white format;
3. Next, take a frame from the video stream and also translate into black and white. This will be our foreground;
4. As the black and white images can be presented as an array of values from 0 to 255 (representing the brightness of pixels), perform subtraction of values of foreground from background. In the absence of new objects in a scene we get a value close to zero. If a scene has a new object we will get to a certain place on the image spot in the form of our object with values significantly greater than 0;
5. The resulting image should be binarized to eliminate unnecessary noise and greater detailing.
6. With proper binarization we get the "spot" of ones in the form of our object. Then these units should be combined into one object is identified in the video such as square;

7. At the end, we should take coordinates of our spot on the last frame to build the trajectory of motion (Fig. 1).

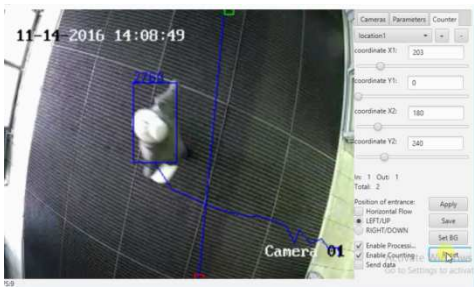

Fig. 1. Demonstration of the algorithm

This algorithm can be implemented using any programming language, but advised to be able to work with streams, was the necessary tools and libraries for image processing and receiving RTSP video streams from IP cameras. The algorithm is not very heavy system and can run on minicomputer such as RaspberryPI and LattePanda.

The problem is that when the lighting on foreground changes, pixels may become lighter or darker. After subtraction and binarization appear extra group of units that the program can be grouped into separate objects. The solution is continuous updating of backgrounds, approximately every 5 seconds. But in this case, on the backgrounds are constantly appears detected objects. The solution is castecne the combination of the new background and the old foreground according to the following algorithm:

1. To form a new background. Every 5 seconds the background becomes the last frame (last foreground with detected objects);

2. Take the coordinates of detected objects from the past foreground and cut parts of picture with these coordinates from the past background;

3. Cut parts paste at the same coordinates on the new background;

4. Carry out further steps to detect moving objects.

Thus, using this algorithm it is possible to minimize errors detects moving objects under changing illumination. This makes it possible to carry out surveillance on the street and do not depend on sudden changes in the weather, motion shading, solar reflections. The method does not lead to a large load on the system and can be integrated into any CCTV or video analytics systems.

УДК 004.7:519.87(043.2)

О. В. Пономаренко, к.т.н.,
Г. О. Булаковська
Національний авіаційний університет, Київ

ІЄРАРХІЧНА СИСТЕМА КОМП'ЮТЕРИЗОВАНОГО УПРАВЛІННЯ ПРОДУКТОПРОВОДАМИ

Традиційно системи автоматизованого (а потім – комп'ютеризованого) управління продуктопроводами будувалися за так званим «острівним» принципом [1]: в рамках великого підприємства трубопровідного транспорту, що складається з різнорідних по специфіці діяльності підрозділів, протяжного трубопроводу, що проходить інколи по декількох регіонах, існують свої функціональні вимоги до систем автоматизації і телемеханізації, застосовуються свої, часто вузькоспеціалізовані інформаційні технології і системи. Крім того, часто окремі структурні підрозділи підприємства мають великий степінь самостійності і вирішують задачі автоматизації і комп'ютеризації на власний вибір, не погоджуючи рішення, що приймаються, з іншими підрозділами. В результаті в рамках підприємства функціонує безліч інформаційних систем різного масштабу і призначення, з устаткуванням різних виробників. Внаслідок цього виникають труднощі узгодження параметрів систем, інтерфейсів і протоколів обміну інформацією. Залишається необхідність ручної обробки інформації на проміжних етапах і на завершальному етапі, що наводить до підвищення трудомісткості, збільшення затримок і додаткових помилок і спотворень. Виходом з ситуації, що склалася, є вживання концепції відкритих систем, стандартизації комп'ютерних і мережних технологій, тобто перехід від «острівного» до «материкового» принципу побудови автоматизованої і комп'ютеризованої системи управління продуктопроводом. необхідно створювати єдину інформаційну систему з ієрархічною структурою. Структура сучасної автоматизованої та комп'ютеризованої системи моніторингу та ієрархічного управління "материкового" типу зображено на рис. 1.

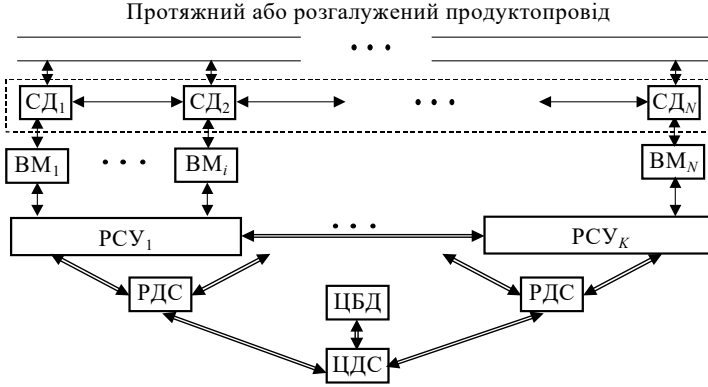

Рис. 1. Структура автоматизованої та комп'ютеризованої системи моніторингу та управління "материкового" типу

$СД_1$ ... $СД_N$ – сенсорні датчики, об'єднані в автономну сенсорну мережу; $РСУ_i$ – районна (регіональна) система управління; РДС – регіональна диспетчерська служба; ЦБД – центральна база даних. Подвійними лініями зображені зв'язки через комп'ютерну мережу.

Структури АСУ ТП можуть бути децентралізованими (розподіленими), централізованими або ієрархічними (розподіленими багаторівневими) [1].

1. Польовий рівень або рівень об'єкту.
2. Нижній рівень або рівень контролерів, у яких здійснюється перетворення сигналів, зв'язок датчиків та виконавчих механізмів з мережним рівнем.
3. Мережний рівень або рівень передачі даних.
4. Верхній рівень або рівень обробки та прийняття рішень.

Ієрархічна багаторівнева система представляє собою симбіоз децентралізованої та централізованої систем управління. У результаті аналізу та досліджень встановлено, що при раціональній побудові та налаштуванні вона поєднує достоїнства попередніх систем та у певній мірі є вільною від їх недоліків.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Пономаренко О. В. Комп'ютеризована система виявлення свищів у продуктопроводах. – Дис. ... канд. техн. наук. Спеціальність 05.13.05 – комп'ютерні системи та компоненти. – К.: НАУ, 2011. – 114 С.

УДК 004.72(043.2)

В. А. Ракицький, аспірант
Національний авіаційний університет, Київ

ПОРІВНЯЛЬНИЙ АНАЛІЗ WEB ТА LOTUS NOTES НА РІВНІ СЕРВЕР - КЛІЄНТ

Пошук актуальних напрямів досліджнь в умовах інформатизації всіх сфер діяльності людської спільности спонукає науковців до розробки ефективних засобів комунікації, основними з яких є комп'ютерні мережі та системи.

Порівнюючи функціонування систем Web та Lotus Notes можна побачити, що вони обидві використовують просту модель клієнт-сервер, але відрізняются документними моделями, які знаходяться в їх основі. На рис. 1 відображена подібність архітектур Web та Notes. В середовищі Web документ представляє собою текстовий файл, в якому містяться команди на мові HTML або XML. В основі ж Lotus Notes лежать списки елементів, так звані нотатки. Нотатка – це структура данних, яка привязана до бази данних.

Взаємодія Notes підтримується за допомогою підсиситеми RPC та електронної пошти, а для Web – пртоколами HTTP.

В обох системах використовується графічний інтерфейс, через браузер, для перегляду інформації. Крім того Notes має спеціальні додатки для редагування заміток. Для обох систем синхронізація загалом локальна та її підтримка мінімальна.

Якщо аналізувати кешування та реплікацію, то кешування в Web ефективніше ніж в Lotus Notes, воно підвищує маштабованість всієї системи. В противагу кешуваню, реплікація грає більш значну роль в Notes, яка здійснюється, наприклад, за допомогою епідемічних алгоритмів зі слабкою формою поширення змін.

Протокол TCP використовується для надійності систем Web, а в Lotus Notes – спеціальні механізми підтримки кластерів серверів Domino. Відновлення системи, в обох випадках, не пристосоване для розподілених систем, та обмежене відновленням одиничного серевера (Notes) або відсутня явна підтримка (Web).

Web організує захищений канал між клієнтом та сервером, використовуючи засоби захисту транстпортного рівня (TLS). Натомість, Notes використовує сертифікати аутентифікаціїї, де для керуванням доступом використовують нотатки, які містять списки

ACL. Ці нотатки відкривають широкі можливості для індивідуального налаштування механізмів контролю доступу.

При об'єднанні протоколів Web з технологією Notes, клієнти Notes використовують власні протоколи для роботи з об'єктним сховищем складних документів, а браузери Web можуть користуватися вбудованою в Notes підтримкою протоколу HTTP і формату документів HTML.

Мультимедійний контент та сценарії потребуть протоколи додатків як для Web та і для Lotus Notes.

В зв'язку з тим, що для зберігання інформації Lotus Notes використовує бази даних, в той час як для Web – файлова модель зберігання, то індиксація теж різна: в Web використовують URN або URL, а Notes – універсальний ідентифікатор (UNID).

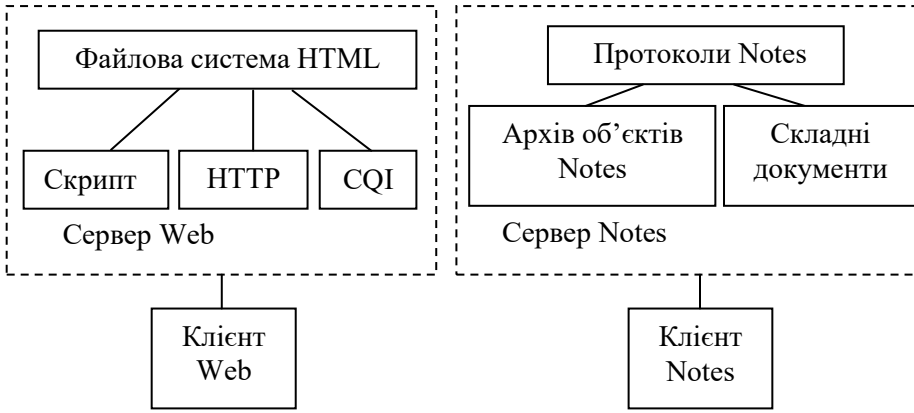

Рис.1. Архітектура середовища Web та середовища Notes

Результати порівняльного аналізу будуть корисними для розробників і користувачів апаратного та програмного забезпечення, в тому числі і для наукових досліджень за тематикою комп'ютерних систем та мереж. Можливий варіант використання в навчальному процесі підготовки фахівців спеціальності "Комп'ютерна інженерія".

УДК 004.738.5(043.2)

В. О. Рудюк,
Національний Університет Харчових Технологій, Київ
Л. О. Ничипоренко
Національний Університет Біоресурсів і Природокористування України, Київ

СИСТЕМА ПРОЕКТУВАННЯ INTERNET ПРОВАЙДЕРА

Якщо говорити про основні елементи технології Internt, то, по-перше, слід відзначити децентралізовану структуру цієї мережі. У світі не існує центрального керуючого органу, який слідкував би за інформацією, яка розміщається в Internet. Дану функцію виконують різні підключені до Internet мережі. Вони й визначають яка інформація буде розміщатися в мережі і як ця інформація буде передаватися. Така повністю розподілена структура робить Internet дуже гнучкою і дозволяє їй підтримувати необмежену кількість користувачів. Однак, підключені до Internet мережі повинні відповідати певним стандартам.

Головним завданням було побудувати обчислювальну мережу для провайдера Інтернет на базі «Укртелеком» м. Вінниця. Дане підприємство надає весь спектр телекомунікаційних послуг. За короткі терміни компанією побудовані нові цифрові АТС, волоконно-оптичні лінії. Все це забезпечило сучасну якість зв'язку, широкий доступ до новітніх телекомунікаційних послуг.

Інтернет-провайдери надають користувачам доступ до мережі Інтернет та інші, пов'язані з Інтернетом послуги.

У число надаваних Інтернет-провайдером послуг можуть входити:

- доступ в Інтернет по комутованих і виділених каналах;
- бездротовий доступ в інтернет;
- виділення дискового простору для зберігання та забезпечення роботи сайтів (хостинг);
- підтримка роботи поштових скриньок або віртуального поштового сервера;
- оренда виділених і віртуальних серверів;
- резервування даних;
- та інші.

Необхідність побудови полягає в тому, щоб забезпечити м. Вінницю і прилеглі мікрорайони доступом в мережу Інтернет та надання пов'язаний з Інтернетом послуг.

Існує безліч технологій для організації доступу абонентів в Інтернет: Ethernet , волоконно-оптичні лінії, бездротові середовища (Wi - Fi , Wi - MAX).

У м. Вінниця є закладена інфраструктура дротового зв'язку, в якості технології доступу в Інтернет була обрана дротова технологія ADSL. Смуга пропускання лінії належить користувачеві цілком. На відміну від кабельних модемів, які допускають поділ смуги пропускання між усіма користувачами (що значною мірою впливає на швидкість передачі даних), технологія ADSL передбачає використання лінії тільки одним користувачем. Технологія ADSL ефективна з економічної точки зору хоча б тому, що не вимагає прокладки спеціальних кабелів, а використовує вже існуючі двопровідні мідні телефонні лінії.

В якості білінгової системи (АСР) на сервері була обрана LANBilling.

Комплекс програм "LANBilling" орієнтований на застосування в розподілених мережах, що складаються з безлічі вузлів, що забезпечують надання послуг абонентам. Вузли можуть являти собою пристрої різного типу: від маршрутизаторів IP-трафіку до абстрактного лічильника послуги, що має одиницю виміру. Послуги різного типу враховуються, контролюються і тарифікуються різними мережевими агентами. Мережевих агентів може бути декілька. Кожен з них фізично може перебувати на різних пристроях і отримувати дані від мережевих компонентів різного типу.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. В. Г. Оліфер, Н. А. Оліфер. Комп'ютерні мережі. Принципи, технології, протоколи: Підручник для вузів. 3-е изд. - СПб .: Питер, 2006. – 958 с.: іл.
2. Конспект лекцій з дисципліни «Мережеві технології»
3. Керівництво по експлуатації LANBiling 1.9
4. Бондаренко В.Г. Технічна експлуатація сучасних цифрових мереж //Радіоаматор. − 2006. − № 2.

УДК 004.451.44

O.V. Rusanova, assistant professor,
A. V. Korochkin, assistant professor
NTUU "Igor Sicorsky Kyiv Politechnical Institute", Kyiv

SCHEDULING PROBLEMS FEATURES FOR MODERN MULTICOMPUTER SYSTEMS

In this paper we consider the main architecture peculiarities of multicomputer systems that belong to list TOP-500 (48th edition) most powerful parallel computers in the world. We define the following main features: huge nodes number; multi-core nodes organization (from 8 up to 256); communications nets types; nodes heterogeneity that connected with using coprocessors for special applications (more than 80 systems); system topology organization. Analysis of the above characteristics shows that on the one hand, the effective use of such systems depends on the scheduling problem implementation quality, and on the other hand for modern systems with a huge nodes number it is much more difficult to provide the quality of the scheduling problem solution. Therefore, the improvement of scheduling methods is a very urgent task today. Usually initial data of scheduling problem performing for multicomputer systems include: task graph, system graph and optimization criterion [1]. Task graph is represented by directed acyclic graph – DAG. In the graph set of vertices and a set of edges are, respectively, processes and information dependencies that means relationships between them. The weight of vertice in the task graph defines the computational complexity of this process. Information dependence between processes is determined by the edge between them in the graph task. Task graph structure defines the order of processes computing in given application. Moreover, before performing each process must receive all necessary data from its predecessor(-s). Data transfer is performed only when the two connected processes assigned to different processors. If they are assigned to the same processor, the communication cost can be ignored and equals to zero. If a process has several predecessors, then applies the operation of logical "AND" to determine the readiness process execution. Process without predecessors called input and process without followers as output. System graph is represented by an undirected graph. In this graph set of vertices and a set of edges are, respectively the processor elements and topology of the

communication channels between them. The vertices weight defines performance of the processor. The weight of edges defines the channel capacity between processors.

In this paper we show that traditional task and system graphs for modern most powerful multicomputer systems are not suitable because of their features. Modification of such graphs are proposed.We represent two types of vertices for task graph, such as: vertices for computational processes (application subtasks) and vertices for special functions (for example, graphic tasks) that run on coprocessors. Edges represent data connections between computational vertices and/or special functions.

In paper we suggest also modification of system graph for modern multicomputer systems. We propose using two levels of system graph. System graph of the first level shows computational nodes and coprocessor communications (topology). For such graphs me can use two vertices types: vertices corresponding computational nodes of parallel computer and vertices corresponding coprocessors for special functions. System graph of the second level shows computational nodes cores relationships. In such graph cores correspond vertices and edges shows connections between cores in system node. Both graphs of the first and second levels are undirected and weighted. Weights of vertices correspond to nodes, coprocessors or cores performances. Weights of edges correspond data transfer rate (throughput) between computational nodes, coprocessors and cores in system.

Usually minimal run time of given application with determined system cost is used as an optimization criterion for scheduling problem solution. Modern multicomputer systems with huge cores number can be used not only for single but also for parallel execution multiple applications. Therefore it's more suitable using the following optimization criterion: minimal system cost that provides minimal run time of given application.

All results this paper can be used for improvement of scheduling methods for modern multicomputer systems.

REFERENCES

1. Русанова О. В. Спосіб планування обчислень для мультиядерних кластерів / О.В. Русанова // Вісник НТУУ «КПІ». Інформатика, управління та обчислювальна техніка: Зб. наук. пр. – К.: Век+, − 2016. – No 64. – С. 31-37.

УДК 004 (043.2)

О. В. Толстікова, к.т.н.
А. Б. Коцюр, асистент
Національний авіаційний університет, Київ

СИСТЕМА ОБРОБКИ ТА ВІДОБРАЖЕННЯ АЕРОНАВІГАЦІЙНОЇ ІНФОРМАЦІЇ

Безпечне та ефективне авіаперевезення забезпечується більш доступної та точної навігацією і збільшенням обсягу спостереження за підтримкою надійних засобів зв'язку, навігації й спостереження в раціонально організованій системі повітряного руху. Для досягнення цієї мети створена та впроваджена аеронавігаційна система з використанням супутникових технологій.

Супутникова система навігації (GNSS — Global Navigation Satellite System) − це комплексна електронно-технічна система, що складається з сукупності наземного та космічного обладнання та призначена для позиціонування в просторі і в часі, а також визначення параметрів руху для наземних, водних та повітряних об'єктів.

Ефективна система обробки та візуального представлення аеронавігаційної інформації з використанням супутникових технологій значно впливає на процес забезпечення ефективного та безпечного управління повітряним рухом та безпосередньо повітряного судна (ПС).

Мережа мультичастотних GNSS-станцій, що працюють у режимі реального часу, дозволяє безперервно отримувати дані радіонавігаційних супутникових вимірювань.

Для збільшення міри точності визначення координат використовуються допоміжні системи функціональних доповнень SBAS (супутникова) і GBAS (наземна) та ABAS (бортова система функціонального доповнення).

Проаналізовані недоліки існуючої системи обробки та відображення аеронавігаційної інформації (COBAI) та визначені вимоги до неї. При виборі архітектури COBAI основними мотивами були: полегшення користування системою для авіаційних споживачів, забезпечення користувачеві мобільності.

Для цих цілей більше підходить архітектура тонкого клієнта, коли в ролі клієнта виступає звичайний веб-браузер.

Розглянути деякі особливості роботи ABAS, пов'язані з необхідністю забезпечення високих характеристик якості функціонування на усіх етапах польоту повітряних суден, що може бути досягнуто тільки за рахунок відповідної реконфігурації структури і параметрів алгоритмів комплексної обробки інформації. Бортові функціональні доповнення підрозділяються на автономной контроль цілісності приймача (RAIM) і цілісності на борту ПС (AAIM).

Згідно вимог до системи та дослідженнями пропонується додаток «RAIM Real Time Service», який дозволяє відстежувати навігаційні дані та відображати їх у реальному часі.

RAIM контролює розрахунок GPS координат місця розташування об'єкту, у разі їх перевизначення. Тобто, у тому разі коли доступні більше супутників, ніж необхідно для визначення позиції, отримані додаткові псевдовиміри мають бути сумісні з розрахованими координатами позиції. Значення отримані від псевдовимірів, які істотно відрізняється від очікуваного значення можуть привести до неправдивого визначення передавального сигнал супутника або іншої проблеми що порушує цілісність сигналу. Автономний контроль цілісності (RAIM) забезпечує цілісність системи GPS моніторингу в авіаційних застосуваннях. Для вирішення цих завдань бортове устаткування супутникової навігаційної системи (СНС) повинне мати функцію RAIM або її еквівалент (AAIM). Основні функції RAIM: функція прогнозу доступності RAIM дозволяє отримати інформацію про можливість використання функції RAIM на території усієї земної кулі; передбачення доступності RAIM по маршруту - дозволяє отримати інформацію про можливість використання функції RAIM на заданому маршруті руху повітряного судна; функція реального часу - забезпечує відображення інформації про поточний стан угрупувань ГЛОНАСС і GPS і цих супутникових систем в зоні дії станцій моніторингу як при автономному, так і при диференціальному режимі роботи бортового устаткування СНС; прогноз RAIM Аеропорт - ця функція дозволяє оцінити доступність функції RAIM для аеродрому, часу і типу польоту, а також використовуване орбітальне супутникове угрупування.

УДК 004.075:004.7 (043.2)

І. І. Феденко, аспірант
Національний авіаційний університет, Київ

АЛГОРИТМ ПІДВИЩЕННЯ ШВИДКОДІЇ АНАЛІЗУ ТРАФІКУ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Розвиток комп'ютерних мереж та широке застосування систем зв'язку передбачає розгляд питань оцінювання якості та надійності роботи систем.

Задачі аналізу трафіку комп'ютерних мереж набули значного поширення в вирішенні проблем забезпечення якості провідного та безпровідного зв'язку, безвідмовної роботи інформаційних ресурсів, інформаційного пошуку [1]. Прогнозування завантаження мережі дозволяє забезпечити надійність роботи, раціональне використання ресурсів мережі, ефективне використання обладнання.

Для підвищення швидкодії аналізу трафіку запропоновано застосування системи попереднього аналізу, що дозволяє системі по двом попереднім вимірам трафіку і певних ймовірнісних параметрів трафіку екстраполювати третє значення трафіку через вказаний інтервал часу [2]. Екстрапольовані значення трафіку зрівнюються з максимально допустимими значеннями для кожного інтерфейсу окремо.

Запропоновано використання розробленого алгоритму автоматизованого попереднього аналізу трафіку між інтерфейсами мережевого обладнання (рис.1), який можна застосовувати в комп'ютерних мережах за певних умов. Даний алгоритм дозволяє прискорити аналіз трафіку.

Розроблена математична модель оцінки можливостей з розподілу і передачі трафіку мережею з автоматизованим балансуванням трафіку. Враховані параметри зовнішнього впливу на роботу всієї системи.

Надалі буде проведено моделювання запропонованого алгоритму.

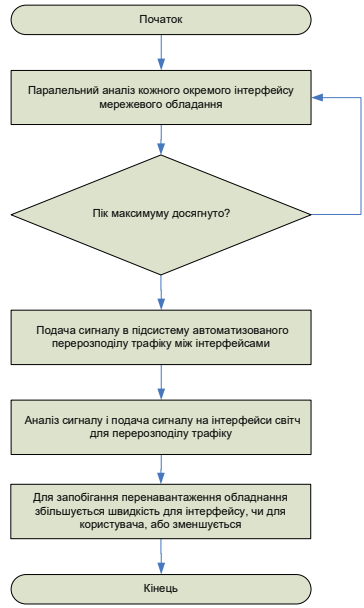

Рис.1. Алгоритм автоматизованого попереднього аналізу трафіку

На основі результатів будуть зроблені висновки щодо його ефективності, а також необхідності доопрацювання та оптимізації параметрів аналізу трафіку. Розглядається можливість використання інших апаратно-програмних засобів для розширення функцій системи автоматизованого попереднього аналізу трафіку.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Zhukov I.A. The algorithms coordinating traffic in computer network / Zhukov I.A., Pechurin N.K., Kondratova L.P., Pechurin S.N // Проблеми інформатизації та управління: Зб. наук. праць. – К.: НАУ, 2016. – Вип.1 (45). – С.31-36.

2. Ігнатов В.О. Метод оптимальної екстраполяції випадкових нестаціонарних сигналів на тлі завад / В.О. Ігнатов, О.В. Андреєв, В.І. Андрєєв // Проблеми інформатизації та управління: Зб. наук. праць. – К.: НАУ, 2010. – Вип. 2(30). – С. 79-83.

УДК 004.056.53

Т. М. Чебаненко, к.т.н.,
Т. А. Руденко
Національний технічний університет України «КПІ ім. І. Сікорського», Київ

ЗАХИЩЕНЕ МОДУЛЯРНЕ ЕКСПОНЕНЦІЮВАННЯ У ХМАРНИХ СИСТЕМАХ

Випереджальний розвиток засобів телекомунікацій і глобальних мереж стимулював появу нової технології комп'ютерної обробки інформації - хмарних обчислень. Хмарні технології передбачають віддалене надання на комерційній основі будь-якому користувачеві комп'ютерних ресурсів з деякого пулу. Разом з тим, можливість використання потужних обчислювальних ресурсів сучасних суперкомп'ютерів, що надаються хмарними технологіями, дозволяють потенційним зловмисникам збільшити ефективність злому існуючих систем захисту інформації у декілька разів. Це вимагає вживання спеціальних заходів для підвищення стійкості протоколів криптографічного захисту комп'ютерної обробки інформації в усіх сферах людської діяльності.

Більша частина сучасних протоколів захисту інформації базується на використанні алгоритмів криптографії з "відкритим" ключем, математичною основою більшості яких є операція модулярного експоненціювання $A^E \bmod M$. Виходом із ситуації може бути використання для модулярного експоненціювання обчислювальних ресурсів хмарних систем, але робити це так, щоб при обчисленні не були в явному вигляді використані секретний код експоненти E і число A, що оброблюється.

Метою досліджень є розробка методу захищеного виконання операції модулярного експоненціювання в хмарних системах з можливістю її розпаралелювання.

Для досягнення поставленої мети пропонується m-розрядний двійковий код експоненти $E=\{ e_0, e_1, ..., e_{m-1}\}$ випадковим чином розділити на h груп $\delta_0, \delta_1,...,\delta_{h-1}$ 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:

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

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. Значення $R_1,...,R_{h-1}$ и $w_1,...,w_{h-1}$ відсилаються до хмари.

3. У хмарі паралельно обчислюються $D_1 = R_1^{w_1} \bmod M$,..., $D_{h-1} = R_{h-1}^{w_{h-1}} \bmod M$ і обчислені значення повертаються користувачеві.

4. Користувач обчислює $A^E \bmod M = (R_0 \cdot \prod_{i=1}^{h-1} D_i \bmod M) \bmod M$.

При обчисленні експоненти $A^E \bmod M$ за класичним алгоритмом [1] середнє число операцій модулярного множення складає $1.5 \cdot m$.

При обчисленні користувачем h кодів за запропонованим способом, кількість операцій модулярного множення зменшується приблизно в три рази за рахунок того, що решта операцій виконується у хмарі паралельно. При наявності у користувача h процесорних ядр обчислення кодів може виконуватись паралельно, тоді кількість операцій модулярного множення зменшується приблизно в $0.75 \cdot h$ раз.

Разом з тим, по кодах R_1, $R_2,...,R_{h-1}$, що передаються у хмару, практично важко відновити секретні коди експоненти E і числа A.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Menezes, A., van Oorschot, P., Vanstone, S.: Handbook of Applied Cryptography.- CRC Press.- 1996.- 780 p.

УДК 004.56.5(043.2)

М. С. Шмайденко
Національний авіаційний університет, Київ

АНАЛІЗ ЗАСОБІВ HONEYPOT ЗА РІВНЯМИ ВЗАЄМОДІЇ ЗІ ЗЛОВМИСНИКОМ

В даній роботі викладено результати аналізу класифікації технології Honeypot за рівнем взаємодії зі зловмисником. Honeypot доповнюють систему захисту інформації в комп'ютерній мережі, але не можуть виступати єдиним засобом вирішення проблеми безпеки. Завдання Honeypot – зазнати атаки або несанкціонованого дослідження. Чим вище рівень протоколювання, тим більшу деталізацію мають записи протоколу програми . Обсяг даних змінюється в залежності від рівня взаємодії. [1] Honeypot зі зловмисником. Метою даної роботи є аналіз класифікації Honeypot за рівнем взаємодії зі зловмисником.

Засоби Honeypot класифікують за рівнем взаємодії зі зловмисником [2]:

- Honeypot першого рівня

Засоби Honeypot першого рівня мають просту структуру і базові функції. Головна мета Honeypot першого рівня - виявлення сканувань і несанкціонованих спроб з'єднання. Через обмежену функціональність, більшість з них реалізуються програмно. Завдання адміністратора безпеки в даному випадку - проводити моніторинг даних, які генерує Honeypot, а також відстежувати зміни імітованого програмного забезпечення. Дані Honeypot мають мінімальний рівень протоколювання і найменший рівень ризику і не можуть бути використані для атаки або дослідження інших систем. Засоби Honeypot цього виду надають інформацію про час і дату атаки; IP-адресу і порт джерела (зловмисник); IP-адреса і порт призначення (Honeypot).

- Honeypot другого рівня

Honeypot другого рівня спроектовані на надання кількох відповідей на дії зловмисника. Зловмисник буде взаємодіяти з Honeypot, що імітує операційну систему, а вся його активність буде контролюватися з боку реальної операційної системи. Однак дане рішення досить складне, що може спричинити появу помилок на стадії налаштування. Тому більшості Honeypot другого рівня не

надають виконання усіх функцій стандартної операційної системи. Такі Honeypot потребують постійної підтримки і і збільшують ступінь ризику, але при цьому здатні отримати набагато більше інформації. Honeypot другого рівня виконує сканування портів, записує активність мережевих хробаків і зловмисників та виконує аналіз стану системи після взлому, а також виконує збір даних про програмні засоби, які зловмисник використовує для атаки.

- Honeypot третього рівня

Засоби Honeypot третього рівня надають великий обсяг інформації про зловмисника. Мета Honeypot третього рівня - надати зловмисникові доступ до реальної операційної системи. Це надає змогу досліджувати нові методи атак, засоби взлому, виявляти нові вразливості в операційній системі. Після отримання зловмисником доступу, він починає взаємодіяти з повнофункціональної операційною системою, яка надає йому можливість здійснювати будь-які дії, наприклад, атаки інші системи або збір трафіку. У більшості випадків Honeypot третього рівня розташовуються в контрольованому середовищі, наприклад, в мережі - після брандмауера, який надає зловмисникові можливість атакувати Honeypot, але забороняє проводити інші атаки. Так як побудована архітектура досить складна, то база правил брандмауера має бути чітко визначена. Підтримка даної системи буде ускладнена оновленням баз правил брандмауера і сигнатур атак системи виявлення вторгнень.

В даній роботі було описано класифікацію технології виявлення атак Honeypot за рівнями взаємодії зі зловмисником.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Lance Spitzner. Honeypots: Tracking Hackers / Lance Spitzner, Addison Wesley – CA, 2005.

2. Roger A. Grimes. Honeypots for Windows / Roger A. Grimes, Apress – CA, 2009

Наукове видання

ЗБІРНИК
ТЕЗ ДОПОВІДЕЙ
X МІЖНАРОДНОЇ
НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«КОМП'ЮТЕРНІ СИСТЕМИ І МЕРЕЖНІ ТЕХНОЛОГІЇ»

(CSNT-2017)

20–22 квітня 2017 року

Тези доповідей надруковані в авторській редакції однією із трьох робочих мов конференції: українською, російською, англійською

Підп. до друку 12.04.17. Формат 60х84/16. Папір офс.
Офс. друк. Ум. друк. арк. . Обл.-вид. арк. 6
Тираж 60 пр. Замовлення № 111-1

Видавець і виготівник
Національний авіаційний університет
03680. Київ-68, проспект Космонавта Комарова, 1

Свідоцтво про внесення до Державного реєстру ДК № 977 від 05.07.2002