

## СТАБИЛИЗАЦИЯ ПРОЦЕССА ВЫБОРА ОПТИМАЛЬНОЙ ТОПОЛОГИИ СЕТИ МЕТОДОМ АНАЛИЗА ИЕРАРХИЙ

В перспективных корпоративных сетях систем УВД должна обеспечиваться поддержка всего спектра услуг, как на уровне транспортных сетей, так и на уровне сетей доступа для терминалов, находящихся в распоряжении оператора. По заявкам клиентов необходимо быстро и без остановки работы системы организовывать и/или модифицировать индивидуальные наборы услуг, в том числе и дополнительные виды обслуживания.

Вследствие многофункциональности систем ОВД возникает проблема многокритериальности оценки её эффективности. Для систематизации критериев, выбора иерархии приоритетов целесообразно применять методы скаляризации вектора показателей, в частности, метод анализ иерархий Саати [1], как наиболее простой и универсальный. Устойчивость решения оптимизационной задачи обеспечивается наличием случайных составляющих различной природы в матрице приоритетов. Они играют роль стабилизаторов решения задачи выбора иерархий, которая относится к задачам на собственные значения матрицы. В табл. 1 приведены элементы матрицы парных сравнений для критериев, по которым определяется наиболее важный критерий.

Таблица 1

Номер параметра $a_i$	I	II	III	IV	$W_i$	$X_i$
I	1	3	5	1/3	1,495	0,306
II	1/3	1	1/3	1/3	0,439	0,090
III	1/5	3	1	1/3	0,669	0,137
IV	3	3	3	1	2,280	0,467
Сумма ( $Y_j$ )	4,533	10,000	9,333	2,000	4,882	1
$(L_{max})_j$	1,388	0,899	1,278	0,934		

Здесь  $W_i = a_i / (a_1 + a_2 + \dots + a_n)$  – веса, которыми определяется относительная важность параметра, а  $X_i = (i^* a_{i2}^* \dots^* a_{in}^*) * (1/n)$  – оценки компонентов вектора собственных значений.

Для обеспечения устойчивости решений предлагается вводить в значения величин парных сравнений малые возмущения случайного характера. При этом матрица парных сравнений перестает быть строго обратнo-симметричной и, соответственно, ее определитель становится не равным нулю.

## Список литературы

1. Саати Т. Принятие решений. Метод анализа иерархий: Пер. с англ./ Т.Саати. – М.: Радио и связь, 1993. – 320 с.

Научный руководитель – Н.А. Виноградов, д.т.н., проф.

УДК 004.73(043.2)

Іванілов Д.О.

Національний авіаційний університет, Київ

**ПОРІВНЯЛЬНИЙ АНАЛІЗ ЗАГРОЗ ПРИ АТАКАХ DDoS ТА BOTNET**

Мережна безпека існує з того самого часу, коли технологія Інтернет отримала комерційний статус. Розглянемо два найбільш вживаних метода мережних атак – *DDoS* та *BotNet*.

*DoS*-атака (англ. *Denial of Service*) – це атака на ресурс з метою припинення його дії. Зазвичай, при відправленні запиту на сайт після *DoS*-атаки, користувач бачить на екрані помилки 404 (не знайдено сторінку) та 503 (сервіс тимчасово недоступний). Атаки поділяються на «зламування» сайту (відправка запиту неправильного виду, що призводить до критичної помилки і видає зловмиснику повні дані ресурсу), недостатню перевірку даних користувача, атаку другого роду (фальшива атака для спрацювання системи безпеки) і, найчастіше, затоплення (перенавантаження ресурсу безглуздими запитамі). Якщо атака ведеться з декількох машин, то її називають *DDoS* (англ. *Distributed Denial of Service*). Найпростіший метод навантажити цільову систему – пінг-запити (запит, що одразу ж відправляється сервером відправнику, показує користувачеві час затримки між відправленням й прийняттям відповіді).

Логічним продовженням розвитку *DDoS* став *BotNet* (англ. *roBot Network*) – та сама технологія, тільки замість користувачів, що свідомо причиняють шкоду ресурсу, використовуються комп'ютери людей, що можуть і не здогадуватись про свою роль у атаці. Останнім на комп'ютер за допомогою віруса-трояна заноситься програма-бот, що активується за «окликом» зловмисника і непомітно від користувача посилає запити на цільову сторінку. Середня мережа інфікованих комп'ютерів складає десятки тисяч машин, найбільша зареєстрована – понад 12 мільйонів. Понад 80% світового трафіка спам-листів складає листування машин у *BotNet*'і заданою рекламою на випадковій адресі.

Ефективних методів протидії мільйонам користувачів, що одночасно відсилають запити на один й той самий ресурс, за визначенням не може існувати. Проте це не означає, що кожен атакований *DDoS*'ом чи *BotNet*'ом сайт неодмінно «рухне». Найбільш ефективними методами протидії атакам на сьогодні є: 1) поширення пропускнуої здатності каналу; 2) приєднання додаткових ресурсів (підключення додаткових серверів для обробки запитів); 3) перенаправлення трафіка на інші сервери за домовленістю; 4) встановлення програмного фільтру на певні види запитів та контратаки по цільових ресурсах атакуючих.

Деякі ресурси мають імунітет до такого роду злочину, бо вони заздалегідь розраховані на велику кількість відвідувачів, або не мають прямого виходу до мережі й працюють через так звані проксі-сервери. Підприємствами з виробництва мережного обладнання йде розробка апаратних засобів протидії атакам, але поки що жоден з винаходів не отримав необхідної підтримки з боку потенційних користувачів.

Науковий керівник – М.А. Віноградов, д.т.н., проф.

## **ИЕРАРХИЧЕСКАЯ МАРШРУТИЗАЦИЯ ПОТОКОВ РАЗНОРОДНОГО ТРАФИКА**

Как известно [1], размер таблиц маршрутов, поддерживаемых маршрутизаторами, увеличивается пропорционально увеличению размеров сети. Требуется большее количество памяти для хранения таблицы и большее время центрального процессора для ее обработки. Возрастает размер служебных пакетов, которыми обмениваются маршрутизаторы, что увеличивает нагрузку на линии. В определенный момент сеть может вырасти до таких размеров, при которых перестанет быть возможным хранение на маршрутизаторах записи обо всех остальных маршрутизаторах. Поэтому в больших сетях целесообразно применять иерархическую маршрутизацию, как это делается в телефонных сетях.

Рассмотрим пример маршрутизации в двухуровневой иерархии с пятью регионами. Полная таблица маршрутизатора состоит из 17 записей. При использовании иерархической маршрутизации таблица, как и прежде, содержит сведения обо всех локальных маршрутизаторах, но записи обо всех остальных регионах концентрируются в пределах одного маршрутизатора, поэтому размер таблицы маршрутов уменьшается с 17 до 7 строк. Чем крупнее выбираются регионы, тем больше экономится места в таблице. Платой за уменьшение размеров таблицы маршрутов является увеличение длины пути. Поэтому оптимальное количество уровней иерархии для подсети, состоящей из  $N$  маршрутизаторов, равно  $\ln N$ . При этом потребуется  $e \ln N$  записей для каждого маршрутизатора. Увеличение длины эффективного среднего пути, вызываемое иерархической маршрутизацией, довольно мало и обычно является приемлемым.

При этом следует различать иерархическую маршрутизацию и сеть с иерархической структурой. В этом случае целесообразно использовать статистический подход с учетом статистики сетевого трафика, в частности, степени его самоподобия. По нашему мнению, достаточно общей оценкой является средняя сложность иерархической маршрутизации для двух узлов, равномерно распределенных внутри автономного (кругового) сегмента с нормированным радиусом. Нормировка осуществляется по физическому расстоянию между узлом-источником и узлом-получателем. Другими словами, можно применять геометрический подход к оцениванию сложности иерархической маршрутизации. При стремлении к бесконечности числа узлов внутри сетевого сегмента ошибка оценивания асимптотически приближается к нулю.

### **Список литературы**

1. Tanenbaum, A.S. Computer Networks, 5<sup>th</sup> Ed. / Andrew S. Tanenbaum, David J. Wetherall. – Prentice Hall, Cloth, 2011. – 960 pp..

*Научный руководитель – Н.А. Виноградов, д.т.н., проф.*

УДК 004.73(043.2)

Модэнов С.Ю.

Национальный авиационный университет, Киев

**МЕТОДЫ ДИСТАНЦИОННОГО УПРАВЛЕНИЯ МОБИЛЬНЫМИ ТЕРМИНАЛАМИ**

В настоящее время все шире применяются методы дистанционного управления компьютером с помощью мобильных терминалов. Функции управления реализуются через беспроводные сети *Wi-fi* или *Bluetooth* в ручном и автоматическом режиме. Также существуют программы для создания пультов управления, предназначенных для «телефонного контроля». Они основаны на использовании «горячих клавиш», позволяют программировать собственные пульты управления и имеют систему поддержки пользователей.

Наибольший интерес представляют следующие сервисные функции.

*Basic Input* – выполняет функцию удалённого тачпада

*File Manager* – позволяет открывать компьютер и просматривать его содержимое.

*Keyboard* – виртуальная клавиатура

*Power* – операции с питанием компьютера (выключение, перезагрузка и др.)

*Slide Show* – для управления мультимедийными презентациями.

*Start* – позволяет получить доступ к программам, расположенным в меню «Пуск»-> «Все программы»

*Task Manager* – выводит на экран список выполняемых программ из диспетчера задач.

*Windows Media Center* – пульт управления *Windows Media Center*.

*Windows Media Player* – пульт управления *Windows Media Player*.

В настройках можно выставить несколько пультов для быстрого переключения между ними: *Preferences* → «*Quick Switch*».

Соединение по *Bluetooth* к компьютеру более удобно в настройке, но дальность действия и стабильность сигнала не так велики, как по *Wi-fi*. По *Wi-fi* можно добиться уверенной передачи сигнала, если завязать подключение на точку доступа или уже имеющуюся локальную *Wi-fi* сеть. В случае наличия и *Wi-fi* и *Bluetooth*, при выходе из зоны действия блютуза вы сможете сменить соединение на *Wi-fi*.

Важной проблемой является обеспечение надежной, а главное – безопасной связи с компьютером. Для решения этой проблемы в первую очередь необходимо реализовать такие функции управления, как авторизация и аутентификация. Второй, не менее важной проблемой является аппаратная реализация метода. Для этого необходимо согласовывать требования к оборудованию объекта управления (удаленного терминала) и управляющего устройства (мобильного терминала). Эта задача, по существу, представляет собой задачу управления, оптимального по быстрдействию, и может решаться методами общей теории управления с учетом специфики рассматриваемой задачи.

Научный руководитель – Н.А. Виноградов, д.т.н., проф.

УДК 004.73(043.2)

Пономаренко А.В., канд. тех. наук

Национальный авиационный университет, Киев

## ВЫБОР ВЕСОВОЙ ФУНКЦИИ АЛГОРИТМА ВЕЕРНОГО ПРЕОБРАЗОВАНИЯ РАДОНА

При определении источников акустических шумов применяются методы дистанционного зондирования с комбинированным (линейным и угловым) сканированием датчиков акустических шумов. Точности можно достичь путем применения методов реконструктивной вычислительной томографии, модифицированных для случая пространственно разнесенных приемников. При обработке данных в области пространственных частот имеем совокупность точек пространственного спектра  $\tilde{f}(p, \theta)$  в полярном растре, т.е. в координатах  $p, \theta$ . Для рассматриваемой задачи наиболее приемлемым методом томографической обработки данных является метод интегрирования фильтрованных обратных проекций [1]. При комбинированном сканировании датчиков для вычисления координат источника утечки необходимо применять обратное преобразование

Радона [2]:  $f(x, y) = \int_{-\infty}^{\infty} \int_0^{\pi} \tilde{f}(p, \theta) e^{2ip(x \cos \theta + y \sin \theta)} d\theta |p| dp$ . По функции  $f(x, y)$  определяется

пространственное положение источника акустического шума, а функция  $|p|$  представляет собой якобиан преобразования при переходе от декартовых координат к полярным. Для уменьшения уровня боковых лепестков предлагается применять вместо функции  $|p|$  сглаженную функцию, в качестве которой выбран модуль первой производной гауссовской функции  $g(x) = a \cdot \exp(-bx^2)$ , где  $a, b$  – константы, выбираемые в соответствии с размерами области интегрирования преобразования Радона. Выражение для весовой функции имеет вид:

$$\left| \frac{d}{dx} [a \cdot \exp(-bx^2)] \right| = ab \cdot |2x \cdot \exp(-bx^2)|. \text{ На рис. 1}$$

изображена пространственно-частотная весовая функция, а на рис. 2 – сечение соответствующей функции  $f_w(x, y)$  точечного источника акустического шума.

### Список литературы

1. Пономаренко А.В. Алгоритм обнаружения и измерения координат источника акустических шумов / А.В.Пономаренко // Наукові записки УНДІЗ. – 2012. – №2(22). – С. 70-75.
2. Хелгасон С. Преобразование Радона / С.Хелгасон. – М.: Мир, 1983. – 152 с.

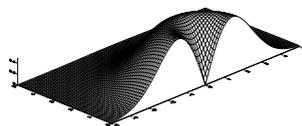


Рис. 1. Весовая функция

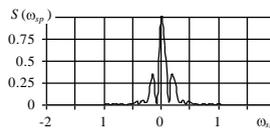


Рис. 2. Отклик точечного источника шума

**ЯКІСТЬ ОБСЛУГОВУВАННЯ В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ**

Невід'ємною частиною підприємства (установи, організації) будь-якої галузі є сучасні інфокомунікаційні технології, які надають транспорт для передачі інформації. Якість функціонування транспортної системи залежить від розвиненості механізмів управління мережею. Сучасні системи управління (СУ) телекомунікаційною мережею (*HP OpenView, IBM Tivoli, Naumen*) дозволяють адміністратору мережі виконувати такі важливі функції як: моніторинг стану мережі, конфігурування окремих мережних вузлів з метою підвищення надійності роботи мережі та оптимізації мережевого трафіку, сегментування завантажених ділянок, складання статистичних звітів.

Аналіз станів мережного середовища ґрунтується на таких інтегральних показниках якості функціонування телекомунікаційної мережі як:

- кількість втрачених пакетів – для *TCP* мережі 1–5% втрачених пакетів, згідно з експертними оцінками, знаходиться в межах норми; 40% втрачених пакетів – граничне значення, при якому мережа практично не працює;

- кількість пакетів, переданих з помилками;
- час затримки доставки пакетів;

- варіація затримки доставки пакетів (джиттер) – особливо важлива для мультимедійних додатків.

Незважаючи на наявні в розпорядженні адміністратора потужні сучасні засоби управління, процес адміністрування залишається трудомістким та складним і багато в чому залежить від інтуїції та досвіду адміністратора. Для підвищення якості управління, пропонується до складу СУ телекомунікаційною мережею інтегрувати елементи штучного інтелекту, наприклад використовувати концепцію «оптимального адміністратора».

СУ мережею повинна швидко реагувати на збої в роботі мережного обладнання та приймати рішення з управління. Досягнення цієї мети можливе за рахунок розподіленої ієрархічної структури. Перший рівень складається з статичних інтелектуальних агентів, розподілених по вузлах мережі. Завдання цього рівня полягає в аналізі станів вузлів та видачі результату цього аналізу другому рівню ієрархії, що дозволяє скоротити службовий трафік. Завдання другого рівня – збір інформації про стан мережі в цілому і прийняття оптимального рішення щодо управління.

Запропонована архітектура СУ дозволяє підвищити надійність та ефективність роботи, як окремих об'єктів комп'ютерної мережі, так і всієї структури в цілому. Крім того, за рахунок прогнозування стану мережі та аналізу ефективності роботи адміністратора можна запобігти появі критичних станів мережі в майбутньому.

*Науковий консультант – М.А. Віноградов, д.т.н., проф.*

**МЕТОДЫ СТАТИСТИЧЕСКОГО СИНТЕЗА ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СИСТЕМ В УСЛОВИЯХ АПРИОРНОЙ НЕОПРЕДЕЛЕННОСТИ**

В процессе создания информационно-коммуникационных систем и сетей необходимо учитывать множество различных условий оптимизации. Часто в качестве критерия оптимизации компьютерной сети выбирают стоимость, а такие критерии, как среднее время задержки передачи сообщений, надежность и т.д., используют в качестве ограничений. Но для сетей масштаба мегаполиса или крупной корпорации данный подход не может дать оптимального решения, т.к. при эксплуатации и модернизации возникают отказы элементов и сбои в работе. Поэтому для таких сетей необходимо учитывать и ряд других критериев: производительность, надежность и безопасность, расширяемость и масштабируемость, прозрачность и безопасность, гибкость и поддержка разных видов трафика, управляемость и совместимость. Среди условий оптимизации и принятия концептуальных проектных решений в формальном отношении иногда предлагают выделить следующие разновидности: условия полной определенности, вероятностно-определенные и условия неопределенности [1]. Эффективнее деление на параметрическую и непараметрическую неопределенность [2]. В первом случае можно сделать предположения об априорных параметрах и параметрах наблюдения (например, статистика сетевого трафика, в частности, степень его самоподобия). Круг априорных распределений сводится к не экспоненциальному семейству (распределениям с «тяжелыми хвостами»). При этом широко применяется байесовский подход. При непараметрической неопределенности приходится задаваться наименее благоприятными распределениями типа распределений с максимальной энтропией и получать некие асимптотические оценки ожидаемой эффективности. Для синтеза системы с оптимальной структурой можно применять минимаксный или адаптивный байесовский подход. Выбор того или иного конкретного метода зависит не только от масштаба информационной системы, но и от круга решаемых с ее помощью задач.

**Список литературы**

1. Сафонова И.Е. Методы формирования и принятия проектных решений в системах автоматизированного проектирования корпоративных компьютерных сетей / И.Е.Сафонова // Известия высших учебных заведений. Поволжский регион. Технические науки. Информатика, вычислительная техника.– 2008.–№ 4.–С.41-49.
2. Репин В.Г. Статистический синтез при априорной неопределенности и адаптация информационных систем / В.Г.Репин, Г.П.Тартаковский. – М.: Сов. радио, 1977. – 432 с.

*Научный руководитель – Н.А. Виноградов, д.т.н., проф.*

УДК 351.814.331:519.711.3 (043.2)

Станко П.А.

Национальный авиационный университет, Киев

**МАТРИЦА КЛЮЧЕВЫХ ПОКАЗАТЕЛЕЙ ФУНКЦИОНИРОВАНИЯ ОПЕРАЦИОННЫХ СИСТЕМ РЕАЛЬНОГО ВРЕМЕНИ**

При оптимизации операционных систем реального времени (ОС РВ) в состав целевой функции входит большое количество основных и дополнительных параметров, от которых зависят ключевые показатели качества сервиса *KQIs*. Оптимизируемыми параметрами задачи являются следующие: оценки топологической и информационной сложности программ  $c_{ii}$ ; оценки надежности программных систем  $c_r$ ; оценки производительности ПО  $c_{sr}$ ; оценки уровня языковых средств  $c_{ij}$ ; оценки трудности восприятия и понимания программных текстов  $c_{per}$ ; оценки производительности труда программистов  $c_{lp}$ ; метрика размера программы по Холстеду  $c_{sz}$ ; цикломатическое число Маккейба  $c_M$ ; сетевые программные ошибки  $c_{ne}$ . В табл. 1 приведены коэффициенты корреляции параметров оптимизации для гипотетической ОС РВ. Данные для расчета взяты из работы [1]. Для расчетов использовалась стандартная программа множественного корреляционного анализа, приведенная в [2].

Таблица 1

Параметр																			
$c_{ii}$		1.0																	
$c_r$		0.76	1.0																
$c_{ij}$		0.52	0.47	1.0															
$c_{sr}$		0.77	0.54	0.39	1.0														
$c_{per}$		0.34	0.28	0.55	0.77	1.0													
$c_{ln}$		0.72	0.91	0.22	0.78	0.46	1.0												
$c_{sz}$		0.38	0.88	0.75	0.72	0.63	0.56	1.0											
$c_M$		0.21	0.19	0.27	0.57	0.41	0.40	0.21	1.0										
$c_{ne}$		0.88	0.91	0.92	0.77	0.66	0.75	0.82	0.46	1.0									
	Коэффициенты корреляции	$c_{ii}$	$c_{ij}$																

Анализ корреляции между основными ключевыми параметрами необходимо проводить с учетом как статистических данных, так и физической природы возникающих ошибок. Результаты корреляционного анализа служат также ключевым индикатором мониторинга и регулирования потоковых данных в ОС РВ. Это необходимо для обеспечения своевременного обмена данными, прогнозирования и предотвращения перегрузок контролируемого сегмента ОС фрагмента. Таким образом, текущий мониторинг и управление уровнем эффективности работы ОС РВ является неотъемлемой частью задачи общего управления качеством сервиса *KQIs*.

**Список литературы**

1. Kreher R. UMTS Performance Measurement: A Practical Guide to KPIs for the UTRAN Environment. - John Wiley & Sons, Ltd, 2006. – 227 pp.
2. Библиотека численного анализа НИВЦ МГУ. Режим доступа: [http://www.srcs.msu.su/num\\_anal/lib\\_na/libnal.htm](http://www.srcs.msu.su/num_anal/lib_na/libnal.htm)

Научный руководитель – Н.А. Виноградов, д.т.н., проф.

УДК 004.73(043.2)

Шевчук Е.И., Каспаревич А. А.

*Национальный авиационный университет, Киев*

## АЛГОРИТМЫ ОПРЕДЕЛЕНИЯ ОРИЕНТАЦИИ КОСМИЧЕСКОГО АППАРАТА С ПОМОЩЬЮ ЗВЕЗДНОГО ДАТЧИКА

В наше время актуальна тема космоса и ориентации в космическом пространстве. Для этого применяются звездные датчики, которые используют программное обеспечение, идентифицирующее сегменты звездного пространства.

Для ориентации КА используется снимок звездного неба. На нем распознаются звездные объекты и их параметры. Данные сравниваются со звездным каталогом и, таким образом, находится месторасположение КА.

Для обработки изображений был разработан алгоритм сканирования двумя окнами с целью упрощения распознавания звездоподобных объектов.

Рассматриваются области для распознавания от маленьких к большим, постепенно получая данные про объект. Организуется проверка на цвет. В результате получаем набор удовлетворяющих нас пикселей, цвет которых влияет на определение звездной величины. Звездная величина – числовая характеристика объекта на небе, чаще всего звезды, которая показывает, сколько света приходит от нее в точку, где находится наблюдатель. Определяется по формуле:

$$A = -2,5\log I + C ,$$

где  $I$  – световой поток от объекта,  $C$  – константа.

Далее реализуется следующий этап алгоритма, который заключается в определении размера и координат области, соответствующей звездному объекту.

Для выполнения операций с данными используется интегральное представление изображений. Оно имеет вид матрицы, размерность которой совпадает с размерностью изображения. Элементы матрицы рассчитываются по следующей формуле:

$$L(x, y) = \sum_{i=0, j=0}^{i \leq x, j \leq x} I(i, j) ,$$

где  $I(i, j)$  – яркость пикселя изображения.

По суммарной яркости окна определяется, есть там объект (его часть), или нет. Площадь объекта находится путем подсчета удовлетворяющих цветовому условию пикселей, которые расположены в пределах границ ранее полученных координат.

Обработанные данные можно использовать для получения информации о звездных объектах, которые необходимы для изучения космического пространства, как на локальном расстоянии, так и при полетах космического аппарата на дальние дистанции с целью определения его местоположения.

*Научный руководитель – В.Н. Опанасенко, д.т.н., проф., проф. Института кибернетики им. В.М. Глушкова Национальной академии наук Украины*