МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЛЕКТРОНІКИ

МАТЕРІАЛИ 23-го МІЖНАРОДНОГО МОЛОДІЖНОГО ФОРУМУ

«РАДІОЕЛЕТРОНІКА І МОЛОДЬ У XXI СТОЛІТТІ»

16 – 18 квітня 2019 р.

Том 4

КОНФЕРЕНЦІЯ

«ПЕРСПЕКТИВИ РОЗВИТКУ ІНФОКОМУНІКАЦІЙ ТА ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНИХ ТЕХНОЛОГІЙ»

Харків 2019

23-й Міжнародний молодіжний форум «Радіоелектроніка та молодь у XXI столітті». Зб. Матеріалів форуму. Т.4. – Харків: ХНУРЕ. 2019. – 126 с.

В збірник включені матеріали 23-го Міжнародного молодіжного форуму «Радіоелектроніка та молодь у XXI столітті».

Видання підготовлено факультетом інфокомунікацій
Харківського національного університету радіоелектроніки

61166 Україна, Харків, прос. Науки, 14
тел./факс.: (057) 7021397

E-mail: mref21@nure.ua

Харківський
національний університет
радіоелектроніки (ХНУРЕ), 2019

Програмний комітет конференції

Снігуров А.В.	к.т.н., декан факультету ІК
Руженцев І.В.	д.т.н., зав. каф. МТЕ
Безрук В.М.	д.т.н, зав. каф. ІМІ
Лемешко О.В.	д.т.н., зав. каф. ІКІ
Захаров І.П.	д.т.н., проф. каф. МТЕ
Павленко Ю.Ф.	д.т.н., проф. ННЦ «Інститут метрології»
Неєжмаков П.І.	д.т.н., генеральний директор ННЦ «Інститут метрології»

ПРОБЛЕМИ ІНФОКОМУНІКАЦІЙ

ВІДМОВОСТІЙКА МАРШРУТИЗАЦІЯ З ПІДТРИМКОЙ БАЛАНСУВАННЯ НАВАНТАЖЕННЯ

Алексин В.В.
Научный руководитель – проф., д.т.н. Лемешко А.В
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Науки, 14, кафедра инфокоммуникационной инженерии, тел. +380958819735, e-mail: undershook@gmail.com

The principle of fault-tolerant routing with load balancing support has been considered and improved. The peculiarity of such networks is that routing protocols with increased levels of fail-safe solutions are used. As shown in practice, this technology is especially needed to maintain multiserviceability. And the use of special protocols can increase the availability of routers performing the role of the gateway by order.

Важливою особливістю сучасних телекомунікаційних мереж (ТКМ), що складають основу глобальної інформаційної інфраструктури, є підтримка мультисервісності. Саме ця функціональність є ключовою при реалізації концепції побудови мереж наступного покоління (Next Generation Network, NGN). Особлива роль в архітектурі забезпечення якості обслуговування (Quality of Service, QoS) з «кінця в кінець» (end-to-end) і особливо при впровадженні мультимедіа-сервісів відводиться засобам широкомовної (broadcast) і багатоадресної (multicast) маршрутизації, що активно використовуються при передачі трафіка таких додатків як IPTV, дистанційного навчання, реплікації баз даних та інформації веб-сайтів, розсилки корпоративної інформації та ін., частка якого в спектрі надаваних послуг постійно зростає [1]. З іншого боку, сучасні протоколи маршрутизації все частіше доповнюються функціоналом підвищення відмовостійкості рішень, прикладом чому може служити поява концепцій Fast ReRoute в мережах MPLS (Multiprotocol Label Switching), а також Fault-Tolerant Routing і IP resiliency technology в IP-мережах.

Продуктивність сучасних ТКМ стрімко зростає, що приводить до з’явлення відмов та перенавантаження мережевого обладнання. Через це великий об’єм даних може бути втрачений, що значно вплине на значення показників якості обслуговування. Тому в транспортних ТКМ, котрі засновані на технологіях IP (Internet Protocol) та MPLS (Multiprotocol Label Switching), використовуються додаткові засоби підвищення відмовостійкості. До таких технологій відносять наступні:

- швидка протокольна збіжність (Fast IGP/BGP Convergence);
- відмовостійка маршрутизація (Fault-tolerant routing);
- швидка перемаршрутизація (Fast ReRoute, FRR).

Технологія відмовостійкої маршрутизації направлена на збільшення доступності шлюзу за замовчуванням і включає в себе такі протоколи:

1. Протокол HSRP (Hot Standby Router Protocol) призначений для збільшення доступності маршрутизаторів виконуючих роль шлюзу по замовчанню. Це досягається завдяки об'єднанню маршрутизаторів в резервну групу з одним IP-адресом, який і буде використовуватися як шлюз за замовченням для комп'ютерів в мережі
2. Протокол VRRP (Virtual Router Redundancy Protocol) призначений для збільшення доступності маршрутизаторів виконуючих роль шлюзу. Це досягається шляхом об'єднання групи маршрутизаторів в один віртуальний маршрутизатор та призначення їм загальної IP-адреси, яка і буде використовуватися як шлюз за замовчуванням для комп'ютерів в мережі.
3. Протокол GLBP (Gateway Load Balancing Protocol) працює аналогічно, але не ідентично іншим протоколам резервування шлюзу, таким як HSRP і VRRP . Ці протоколи дозволяють декільком маршрутизаторам брати участь у сконфігурованій віртуальній групі маршрутизаторів із загальною віртуальною IP-адресою.
4. Протокол CARP (Common Address Redundancy Protocol) мережевий протокол, основним завданням якого є використання однієї IP-адреси кількома хостами в межах сегмента мережі. CARP є вільною, безпечною (в тій мірі, в якій взагалі можна говорити про безпеку протоколу ARP) альтернативою протоколам VRRP і HSRP. CARP дозволяє виділити групу хостів у тій частині мережі і призначити їй один IP-адреса. Така група називається «redundancy group» (група надмірності). В межах цієї групи один з вузлів стає «головним», а решта позначаються як «резервні». У кожен момент часу майстер-хост відповідає на ARP-запити до призначеного IP-адресою і обробляє трафік, що йде до цією адресою. Кожен хост одночасно може належати до декількох груп.

Для підвищення оперативності реагування на можливі відмови в обслуговуванні пакетів, викликані перевантаженням каналів і черг маршрутизаторів, все частіше використовується засоби відмовостійкої маршрутизації [2]. При цьому важливо, щоб протокол маршрутизації забезпечував різноманітні схеми резервування ресурсів та елементів мережі: захисту каналу, вузла, шляху, та навіть шлюзу.

Список використаних джерел:

1. Вегешна Ш. Качество обслуживания в сетях IP. – М.: Издательский дом «Вильямс», 2003. – 368 с.
2. Лемешко А.В. Модель отказоустойчивой маршрутизации многоадресных и широковещательных потоков в MPLS-сети / А.В. Лемешко, К.М. Арус // Системи обробки інформації. – №9 (116). – 2013.

ЗБІР ДАНИХ З ЕНЕРГОЕФЕКТИВНИХ ПРИСТРОЇВ НА ОСНОВІ ШЛЮЗУ З MQTT

Афанасьєв Ю.В.
Науковий керівник – д.т.н., проф. Лемешко О.В.
Харківський національний університет радіоелектроніки
61166, Харків, просп. Науки,14, каф. Інфокомунікаційної інженерії
e-mail: afvv74@ukr.net, тел. (066) 771-56-38)

The system consists of the ATmega328P microcontroller and radio module NRF24L01 +. Separate attachments can be connected with one another, transfer this data, respond to the received information. The systems defines the data. It is necesseary to insert gateway in the main scheme for external control. The gateway consists of the esp8266 controller and the radiomodule NRF24L01+. It perform such functions: collection of information, its saving and transfer for system operation. When will gate receive information, it transfer this information for its accumulation and cloud computing. The gateway use the mqtt-protocol for transfer information to other devices, which are the elements of the net.

Функціонування об’єктів інфраструктури залежить від дотримання правил експлуатації та мір безпеки, що попереджує виникнення нештатних ситуацій. З цією метою виникає необхідність в отриманні інформації про стан обєктів. Отримання даних забезпечується за рахунок побудови оптимальної схеми збору, обробки, передачі, аналізу інформації, що дозволяє своєчасно виявити та локалізувати критичну ситуацію.

Дослідження функціональних схем складних технічних систем, показує, що для контролю певних параметрів не має потреби в безперервному використанні датчиків для збору даних, що дозволяє зменшити енерговитрати. Для забезпечення контролю параметрів автономних систем актуальним є застосування пристроїв, що мають низьку енерговитрату. Таким чином, дослідження спрямовано на пракичну реалізацію мережі з пристроями, що мають низьку енерговитрату. Особливостями, які необхідно враховуати є: обмеження по функціонуванню каналів зв’язку та по автономному жівленню. Запропоновано фіксувати дані через заданий інтервал часу або по зовнішньому перериванню.

Система включає мікроконтролер ATmega328P та радіомодуль NRF24L01+. Алгоритм роботи забезпечує обмін даними між окремими елементами, що дозволяє розглядати систему, як «деценралізовану систему збору, обміну та управління даними». Зовнішній контроль данихздійснюється за рахунок використання шлюзу. Шлюз складається з контролеру esp8266, радіомодулю NRF24L01+. Він забезпечує реалізацію функцій: збір та збереження даних, передача інформації по запиту. Після

отримання інформації шлюз забезпечує її передавання для накопичення, для хмарних обчислень або ретрансляції для інших пристроїв на основі протоколу MQTT. MQTT-протокол забезпечує реалізацію проектів в концепції Інтернет Речей (IoT-решення). Протокол харакеризується невеликою кількістю механізмів захисту, однак всі його реалізації підтримують сучасні стандарти безпеки (наприклад SSL/TLS). Розглянемо варіант мережи, що включає пристрої на яких розашовані датчики: руху, температури та ін. і релє, за допомогою якого здійснюється керування параметрами електромережі. Використання шлюзу дозволить відображати зібрану інформацію в мережі в web-інтерфейсі.

Сучасною технологією передачі даних є протокол LoRaWAN – апаратний протокол управління зв'язком між LPWAN-шлюзами та кінцевими вузлами пристроїв. Пристрої асінхронно передають дані для подальшого відправлення на шлюзи, які відправляють пакети даних на ценралізований сервер мережі, а від нього – на сервери додатків.

Таким чином, застосування шлюзу забезпечує формування різних варіантів обробки даних. Шлюз є ефективним пристроєм для підготовки даних з пристроїв малої потужності перед відправленням їх для подальшого збереження, обробки.

Використані джерела:

1. Кравченко Ю. В. Концептуальний підхід до синтезу складних технічних систем з динамічною структурою / Ю. В. Кравченко, Р. А. Миколайчук // Сучасні інформаційні технології у сфері безпеки та оборони. – 2012. – №2(14). – С. 31-36.

2. Афанасьєв Ю.В. Шляхи забезпечення функціональної стійкості системи конролю та управління доступом до режимних об'єктів / Ю.В. Афанасьєв, Д.В. Сумцов // Проблеми кібербезпеки інформаційно-телекомунікаційних систем: Збірник матеріалів доповідей та тез; м. Київ, 23-24 березня 2017 р.; Київський національний університет імені Тараса Шевченка. - К.: ВПЦ «Київський університет», 2017.- С. 8–13.

3. Афанасьєв Ю.В. Програмно-апаратна реалізація автономної системи контролю доступом / Ю.В. Афанасьєв // 21-й Міжнародний молодіжний форум «Радіоелектроніка та молодь у XXI столітті». Зб.матеріалів форуму. Т.4. – Харків: ХНУРЕ. 2017. – С. 27.

4. Афанасьєв Ю. В. Застосування безпілотних літальних апаратів, як мобільного шлюзу в концепції IoT для системи контролю і управління доступом / Ю. В. Афанасьєв, О.М. Сітков, В.В. Афанасьєв // Проблеми розвитку глобальної системи зв'язку, навігації, спостереження та організації повітряного руху CNS/ATM: тези доповідей науково-технічної конференції, м. Київ, 21-23 листопада 2018 р., Національний авіаційний університет – К.: НАУ, 2019.– С. 3

ВДОСКОНАЛЕНИЙ КОМУТАТОР АНТЕН КВАЗІДОПЛЕРІВСЬКОГО ПЕЛЕНГАТОРА

Білокурова А.О.
Науковий керівник – к.т.н., доц. Філіппенко О.І.
Харьківський національний університет радіоелектроніки
(61166, Харків, пр. Науки,14, каф. ІКІ, тел. (057) 702-13-26),
e-mail: anastasiia.bilokurova@nure.ua, тел. (057) 702-13-26

The method of antennas switching in which the smooth transition from the previous antenna to the next antenna is provided. This method of antennas switching is significantly improve the waveform at the output of the phase detector of the direction finder receiving path, that is improve the accuracy of the determination of the incident signals arriving angle.

Сучасний розвиток суспільства характеризує широке та все більш зростаюче використання радіотехнічних пристроїв. Це призводить зростання взаємних завад та перешкод. Задля усунення радіоперешкод необхідно мати інформацію про місце знаходження радіотехнічних пристроїв та можливих місць виникнення витоку радіохвиль. Актуальним є використання пеленгаторів і при проведенні морських пошуково-рятувальних операцій, наприклад, для визначення місця знаходження джерела сигналу системи Cospas-Sarsat. Для цього необхідно визначити місця розташування аварійних буїв за допомогою радіопеленгатора [1].

На даний час, не зважаючи на велику кількість розробок у цій сфері, є актуальною розробка широкодіапазонних пеленгаційних систем, що є доступними широкому загалу. Розробками таких систем займаються компанії «Rohde & Schwarz», «Moog Fernau Limited», «ОКБ МЕІ», і багато інших [2, 3, 4].

Методи, покладені в основу пеленгування, можна умовно розділити на три групи: амплітудні, інтерферометричні, допплерівські [5]. Останні є фазовими методами. Інструментальна точність фазових пеленгаторів залежить від величини бази (Б) та стабільності зсуву фаз. Для збільшення точності вимірювання кута необхідно збільшувати Б/λ, де λ – довжина хвилі , але тоді результат відліку кута стає багатозначним. Багатозначність можна усунути створенням системи, в якій є декілька антен, з базами $Б_1$,$Б_2$ що поступово зменшуються.

Значною перевагою фазового пеленгатора є можливість повністю уникнути пошуку, оскілки незалежно від напрямку на об'єкт, відлік кута можливий миттєво. Разом з тим необхідно відзначити, що фазовий пеленгатор, може давати додаткові помилки через відбиття радіохвиль від місцевих предметів, що оточують антенне поле. Однак фазові пеленгатори є дорогими, громіздкими та енергоємними.

Для вирішення достатньо широкого класу задач є придатними пеленгатори, яки використовують метод Доплера. Для реалізації цього методу необхідно забезпечити швидке обертання антени. Механічні приладі обертання антени не є сучасними та замість них застосовуються електронні методі послідовної комутації антен, які розташовані по колу.

При звичайному методі комутації антен ефект обертання моделюється послідовної вибіркою дискретної кількості антен, тому на виході демодулятора насправді є серією піків.

Ці піки утворюються під час переходів від однієї антени до іншої в результаті різкої зміни фази сигналу. Частота є мірою швидкості зміни миттєвої фази сигналу, тому раптова зміна фази виглядає як раптова зміна частоти. Смуговий фільтр згладжує піки.

У роботі запропоновано метод комутації антен при якому забезпечується плавний перехід з попередньої антени на наступну. Такий спосіб перемикання антен дозволив значно покращити форму відгуку на виході фазового детектора приймального тракту пеленгатора та точніше реконструювати синусоїдальну форму сигналу для порівняння з еталонним сигналом, що в цілому покращило точність визначення кута надходження сигналу що пеленгується. Зі згладженого сигналу процесор визначає перетин нуля сигналом і також відстежує кутове положення псевдорухомої антени, яке вважається гладко мінливим.

Розроблено електричну схему та побудовано фізичну модель комутатора на основі використання p-i-n діодів, ПЛИС компанії ALTERA та цифро-аналогового перетворювача.

ПЕРЕЛІК ПОСИЛАНЬ

1. Каталог контрольно–измерительного оборудования [Электронный ресурс]. – Режим доступа: www.linetest.ru
2. Moog Inc. high–performance systems catalog [Electronic resource]. – Access Mode: http://www.moog.com/products/navigation-surveillance-systems/direction-finding-df-/
3. Электронный каталог оборудования для радиомониторинга компании Rohde&Schwarz [Электронный ресурс].– Тип доступа: http://www.rohde–schwarz.com.ua/products/radiomonitoring/direction_finder/
4. Рембовский А. М., Радиомониторинг задачи, методы, средства [Текст] / Под редакцией А М. Рембовского, А. В.Ашихмин, В. А. Козьмин –М.: Горячая линия – Телеком, 2006. – 492с. – ISBN: 5–93517–326–3
5. Пат. 4845502 США, МКИ G01S3/46, G01S3/52 Методы и устройство определения направления [Текст] / James L. Carr, Marvin S. Maxwell. – № 178976; заявл. 07.04.88; опубл. 04.07.89. – 7 с.

РОЗВИТОК ТРАНСПОРТНИХ МЕРЕЖ ПАКЕТНОЇ ПЕРЕДАЧІ ДАНИХ

Ведмедеря М.А.
Науковий керівник – к.т.н., доцент, доцент кафедри інфокомунікаційної інженерії, Токар Л.О.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. ІКІ, тел.: 702-13-20)
E-mail: 1231maks@gmail.com

In a hierarchical telecommunications network the backhaul portion of the network comprises the intermediate links between the core network, or backbone network, and the small subnetworks at the edge of the network. In contracts pertaining to such networks, backhaul is the obligation to carry packets to and from that backbone network. A business definition of backhaul is the commercial wholesale bandwidth provider who offers quality of service (QOS) guarantees.

На сьогоднішній день помітно затяте розростання мереж, що диктує негайну потребу в їх модернізації. За останні кілька років різко зріс обсяг переданої та прийнятої інформації, значно збільшилася кількість одночасно працюючих мереж і абонентів в них, з'явилася потреба в подальшому збільшенні швидкості передачі інформації. Одним з можливих рішень даних проблем є створення мереж широкосмугового доступу з використанням різних технологій. Так само не варто нехтувати тим, що саме бездротові технології дають більше можливостей використання мережі. Однією з первісних технологій, яка може задовольнити вищезгадані вимоги є LTE. Технологія 4G (LTE) стрімко ввійшла в життя українців та зайняла свою нішу, хоча й розпочала свій шлях ще з 2015 року від приказу президента про введення даної технології.

Метою публікації є огляд моделі мережі backhaul з використанням технології LTE.

З огляду на вище зазначені вимоги до побудови мережі, а також вимоги масштабованості, гнучкості, керованості і безпеки, розглянемо можливу модель розвитку мережі до рівня ядро / агрегація, відповідно до концепції Unified MPLS Mobile Transport.

Найбільше підходящою топологією до мереж даного типу є топологія Hub and Spoke. Це традиційна зіркоподібна топологія для мереж 2G і 3G з обмеженим числом користувачів і являє собою структуру побудови, де всі елементи ядра розміщені в центральному вузлі. Ця топологія є розширеною модифікацією топології клієнт-сервер. Яка й знаходиться в основі розглянутої моделі.

Опорна мережа оператора складається з трьох рівнів. На рівні доступу вузли CSG, так звані вузли пре – агрегації, працюють в домені RAN. Рівні агрегації і ядра об'єднані в один рівень – агрегація + ядро.

Відповідні йому вузли – вузли агрегації (AGN) і вузли ядра (CN, CN-RR і MTG). Кілька прилеглих базових станцій будуть підключені в один вузол доступу. На всіх рівнях мережі налаштовується протокол MPLS. Система налаштована для одночасної підтримки декількох поколінь мобільного зв'язку в єдиній конвергентній мережевій архітектурі.[3] Забезпечується впровадження LTE з підтримкою Pseudowire Emulation (PWE) для передачі 2G GSM, L2VPN для 3G UMTS / IP і L3VPN для 3G UMTS / IP і LTE. Підтримуються: синхронізація, високі показники якості обслуговування (QoS), протоколи OAM (експлуатації, адміністрування і обслуговування), швидка збіжність і управління продуктивністю. Система оптимізована для підтримки вимог стандарту 4G, таких як IPSec і аутентифікація, пряме з'єднання між eNodeB по інтерфейсу X2, мультикаст, віртуалізація, можливість розподілу EPC шлюзів і балансування трафіку. Об'єднані рівні агрегації і ядра в один рівень (Core + Aggregation) інтегруються в єдиний IGP / LDP домен. Рівень доступу, так званий вузол попередньої агрегації (RAN), складається з окремого IGP домену.[1]

Вузли агрегації об'єднують мобільні мережі рівня доступу протоколом MPLS і роблять їх частиною однієї автономної системи (AC) з мережею агрегації / ядра. Вузли доступу включаються за допомогою різних інтерфейсів до відповідних їм L3VPN. Ці ж L3VPN присутні на вузлах, до яких підключені MSS / RNC і ін. Таким чином, зв'язок між базовою станцією і зазначеними мережевими елементами здійснюється ізольовано всередині L3VPN за допомогою протоколу MPC – BGP.[2]

Таким чином, на підставі концепції Unified MPLS Mobile Transport отримана модель мережі з уніфікованим доступом до рівня ядро / агрегація. Спостерігається необхідність інтеграції об'єднаних рівнів агрегації і ядра в єдиний IGP / LDP домен. Таке рішення в поєднанні з протоколом BGP використовується для сервісів масштабу мережі, а iBGP використовується для отримання IPv4 + label віддалених сервісних точок адміністрування.

Література

1. Токар Л. О., Білоусова К. Е, и др. «Разработка модели опорной сети на основе технологии long term evolushion.» // Восточно-Европейский журнал передовых технологий – 2017.

2. Saranya, B., Muruganandham, S. Mobile Backhaul Network in wireless Sensor [Text] / B. Saranya, S. Muruganandham // International Journal of Engineering Research and General Science. – 2015. – vol. 3. – p. 394 – 397.

3. Muthukrishnan, K. RFC 2917. A Core MPLS IP VPN Architecture [Text] / K. Muthukrishnan, A. Malis. – September 2013. – 348 p.

АНАЛІЗ ВИКОРИСТАННЯ СИСТЕМИ УПРАВЛІННЯ CRM

Волощенко П.В.
Науковий керівник –доц. Сабурова С.О.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. інфокомунікаційної інженерії,
тел. (095) 640-63-17), pavlo.voloshchenko@nure.ua

Customer Relationship Management (CRM) is a relationship management system clinging to. Technology focused on optimizing mutual owner-owned organization with organization. "In essence, it can be made easier and automate the business processes of the company, the robotic organization, as effective as possible.

CRM – система управління взаємовідносинами з клієнтами. Технологія, орієнтована на оптимізацію взаємовідносин своїх клієнтів з організацією. Її основне призначення покращувати і автоматизувати бізнес-процеси компаній, робити роботу організації максимально ефективною. Робота CRM грунтується на використанні управлінських і інформаційних технологіях, застосування яких дає організації побудувати взаємовигідні відносини зі своїми клієнтами. Результатом застосування системи є підвищення і конкурентоспроможності і збільшенням прибутковості організації.

Сам термін CRM-системи з'явився і став набирати популярність в середині 90-х років XX століття. В ті часи, коли набирала зростання глобальна конкуренція. Коли аналогічні товари у різних компаній перестали відрізнятися в якості. Так само розвиток комп'ютерних технологій, які дозволяли збирати, обробляти і аналізувати дані про клієнтів, де кількість клієнтів не грало ніякої ролі. Тоді компанії і стали міняти свої стратегії розвитку, роблячи акцент не на товар, а на клієнта, якому необхідна продукція.

CRM системи використовувалися дуже давно і найпершими і простими системами були у вигляді книг, які могли підняти давню історію про клієнта, а також в майбутньому звернути на нього більше уваги і дати зрозуміти, що він нього пам'ятають постійно. Це дозволяло якомога менше втратити старих клієнтів і залучати нових. Особливу популярність набували компанії малого бізнесу, які розвивалися в сфері послуг. Так як саме CRM давали швидкий і менш витратний зростання ефективного бізнесу. Орієнтація на клієнтів давала таким компаніям зростання конкуренції, утримання клієнтів і стабільний дохід.

У 1987 році була випущена перша комп'ютерна програма, головною цілю, якій було управління контактами. Її засновник Салліван Пет, що дав їй назву «ACT». В даний час існує більше тисячі подібних програм, що відносяться до класу CRM.

В Україні впровадження CRM вперше відбулося в 1989 році. Впроваджувалися вони в банки і фінансовий сектор. Система була західної і навчання в ній могли виробляти на той момент лише західні фахівці, що могли дозволити лише дуже великі українські компанії. CRM системи на ринку вже близько тридцяти років, і до цих пір стоїть питання про перелік їх

функціональної складової. Більшість фахівців з CRM системам кажуть, що програмний продукт повинен мати 11 складових компонентів управління: управління контактами; управління маркетингом; управління фінансами; управління співробітниками; управління документообігу; управління проектами; управління клієнтською базою; управління сховищем інформації; управління аналітичними інструментами; управління контролем і звітністю; управління обслуговуванням.

На сьогодніщній день класифікують CRM системі за наступними типами: операційний тип CRM, головним завданням якого є автоматизувати бізнес-процеси, в яких задіяний контакт клієнта з організацією. Автоматизує маркетингові дослідження, продажу та обслуговування клієнтів. Аналітичний, основне завдання якого полягає в пошуку, аналізі, накопичення, обробки інформації та взаємодія доступу до даних з іншими співробітниками, які накопичуються в протіканні бізнес-процесу. Спільний, що включає в себе використання спільних сервісів та інфраструктури, щоб зробити можливим взаємодія компанії з її численними каналами. Цей тип CRM полегшує взаємодію між клієнтами, підприємством і його співробітниками.

При цьому питання забезпечення якісного функціонування CRM надзвичайно важливий; для цього необхідний комплекс технічних заходів щодо реалізації політики обслуговування CRM, а також система контролю і управління якістю.

Таким чином, сучасні CRM-системи здатні багато в чому спростити життя фахівцям з продажу та маркетингових аналітикам. Звичайно, до цих пір існує ряд моментів, які розробникам ще належить допрацювати, - наприклад, мінімізувати час, необхідний користувачам для введення даних вручну, і поліпшити інтеграцію CRM-додатків с іншими інструментами. Але, швидше за все, це питання часу, який розробники вже успішно вирішують, в тому числі, за допомогою методів штучного інтелекту.

Список використаних джерел

1. Багатоканальний електрозв’язок та телекомунікаційні технології (Ч.2) / Лемешко О.В., Лошаков В.А., Поповський В.В., Сабурова С.О., Епишкин С.О. – Х.: ТОВ «Компанія СМІТ», 2018р.р.. – 482 с. 2. Андерсон К. Менеджмент, ориентированный на потребителя: CRM-технологии как основа новых отношений с клиентом: [Пер. с англ.] К. Андерсон, К. Керр; Пер. А. Успенский. - М.: 2003. - 288 с.

УПРАВЛІННЯ РЕСУРСАМИ ДОСТУПУ ДО MULTI PLAY ПОСЛУГ

Волокітіна О.І.
Науковий керівник – Сабурова С.О.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. Інфокомунікаційної інженерії,
тел. (057) 702-13-20) e-mail: lemur-97@mail.ru факс (057) 702-13-20

The creation of the NGN network reflects the evolutionary development of existing infocommunication networks through the convergence of networks and technologies while providing a wide range of services: from basic services to a variety of Multi play services, which ensures the requirements for efficient management of access resources and the ability to respond promptly to the increasing demands of bandwidth and quality of provision Multi play services.

Інфокомунікаційні технології на сучасному розвитку суспільства виступають основними факторами розвитку світової економіки. Нові технології завойовують світовий ринок і дозволяють створити єдине інформаційне суспільство, де географічні кордони втрачають своє значення як економічний фактор. Для побудови глобальної інформаційної інфраструктури і забезпечення потреби операторів мереж зв’язку для надання щоденно зростаючого різноманіття інфокомунікаційних послуг на базі нових та інноваційних технологій та розширення спектру послуг, що надаються з виконанням нових функцій: «розумні» мережі та мережі «речей», необхідна нова інфокомунікаційна мережа, для забезпечення: швидкого, дешевого створення і впровадження нових послуг для збільшення абонентської бази, зменшення витрат на обслуговування мережі, підтримку користувачів; обробки лавинного об’єму трафіку, узагальненість глобальної мобільності користувачів і послуг зв’язку.

Достоїнства мереж інфокомунікацій, а саме NGN мережі, на базі яких розгортаються мережі майбутнього. Однією з основних позитивних характеристик NGN є розв'язка між послугами і транспортуванням, що дозволяє пропонувати їх окремо і розвивати незалежно, тому в архітектурі NGN має бути чітке розділення між функціями обслуговування і функціями транспортування.

В транспортному шарі NGN застосовуються усі типи мережних технологій, проте перевага віддається технології IP з підтримкою високої якості обслуговування.

Контролери сигналізації в мережі NGN винесені в окремі пристрої для обслуговування декількох вузлів комутації; загальні контролери створюють єдину систему комутації, розподілену по мережі для спрощення алгоритму встановлення з'єднань, і є найбільш економічним для операторів і постачальників послуг.

Запровадження Softswitch дозволяє змінити традиційно закриту структуру систем комутації, бо надає відкриті стандартні інтерфейси між трьома основними функціями: комутації, управлінням обслуговування викликів, послуг та додатків, і дозволяє узгоджувати різні протоколи сигналізації.

Архітектура управління послугами NGN реалізує: підтримку багаточисельних технологій доступу за рахунок гнучкої конфігурації мережі; розподільне управління на основі принципу розподільної обробки в пакетних мережах; відкрите управління для мережевих інтерфейсів при підтримці процесів створення нових і змінення існуючих послуг та їх конвергенція.

Конвергенція – це об'єднання всіх напрямків інфокомунікацій для вигідного використання ресурсів безшовного зв’язку з метою надання широкосмугових нових базових послуг - Multi play. Мережі фіксованого та мобільного зв'язку можна розглядати як конвергентні, бо останні виникли для обслуговування трафіку мови і їх еволюція пов'язана з можливостями базових послуг Multi play .

Перехід від вертикальної до горизонтальної моделі організації та об'єднання різних базових послуг Multi play на рівні транспорту і доступу - це важливий крок на шляху до конвергенції мереж.

Послуга Multi play, яка зображена на рис. 1, це комбінація п'яти послуг: фіксованої телефонії, мобільного зв'язку, мобільного та стаціонарного інтернету і цифрового телебачення IPTV. Multi play – це крок вперед в сфері послуг IPTV

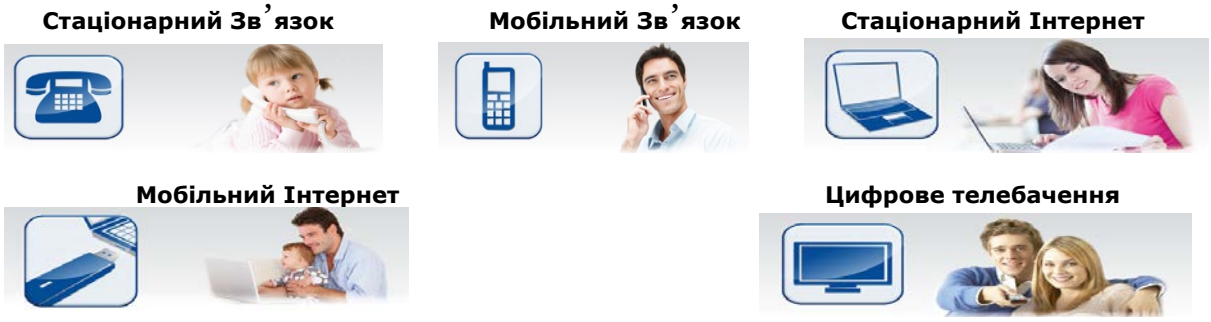


Рисунок 1 – Multi play – комбінація 5 послуг

Створення мережі NGN відображає еволюційний розвиток існуючих інфокомунікаційних мереж за рахунок конвергенції мереж і технологій при забезпеченні широкого набору послуг: від базових послуг до різноманітних послуг Multi play, що забезпечує вимоги до ефективного управління ресурсами доступу та можливість оперативно реагувати на зростаючі потреби пропускної здатності та якості надаваємих послуг Multi play.

МОДЕЛЬ СБОРА ИНФОРМАЦИИ В КЛАСТЕРНОЙ БЕСПРОВОДНОЙ СЕНСОРНОЙ СЕТИ

Галкин П.В.
Научный руководитель – к.т.н., проф. Ключник И.И.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Науки,14, каф. ПЭЭА, тел. (057) 702-14-94)
E-mail: galkinletter@ukr.net

The paper analyzes the cluster structure of wireless sensor networks. The optimal position of the aggregator in the piconet is determined at the site of the intercluster gateway. This position allows the aggregator to communicate with at least two within the piconet. Aroaches for managing information flow in clusters, piconets and between them are proposed.

Беспроводная сенсорная сеть (БСС) – представляет собой распределённую в пространстве систему, важным аспектом работы БСС является ее структура [1]. В работе предлагается кластерная структура беспроводной сенсорной сети. Важным вопросом работы узлов БСС являться энергопотребления узлов [2].

В работах [1-3] приведены подходы для построение БСС с применением кластеризации. Отличием от классической кластеризации является наличие межкластерных шлюзов. Радиус действия и радиус радиосвязи узла могут различаться больше или меньше зоны радиовидимости. Это означает, что два соседних узла могут не иметь возможности обмениваться информацией напрямую, даже если радиусы действия их сенсоров пересекаются.

Радиус действия и радиус радиосвязи только частично описывают возможный процесс сбора информации в БСС [4]. Для рационального использования кластерной структуры в пикосети (части сети) для зоны Z необходимо ввести понятие производного радиуса кластера[4].Такой радиус показывает зону действия кластера, в рамках которой ГУК может получить данные с узлов через определённое количество промежуточных узлов w. Определить производный радиус кластера можно из выражения (1):

$$R'_w(\overset{\Theta}{N}_n(CID)) = R_{radio}(\mathrm{Nj}) + R(CHL(CID)), \qquad (1)$$

где $\overset{\Theta}{N}_n(CID)$ – номер пикосети с идентификатором кластера в этой сети; $CHL(CID)$ – идентификатор ГУК в пикосети.

Процесс сбора данных со всей пикосети осуществляется в рамках зоны Z (рис. 2), которая определяется суммой площадей или объемов (в трехмерном пространстве) зон кластеров и зависит от количества кластеров, что входят в пикосеть, а также от выбора принципа формирования производного радиуса кластера R'_w.

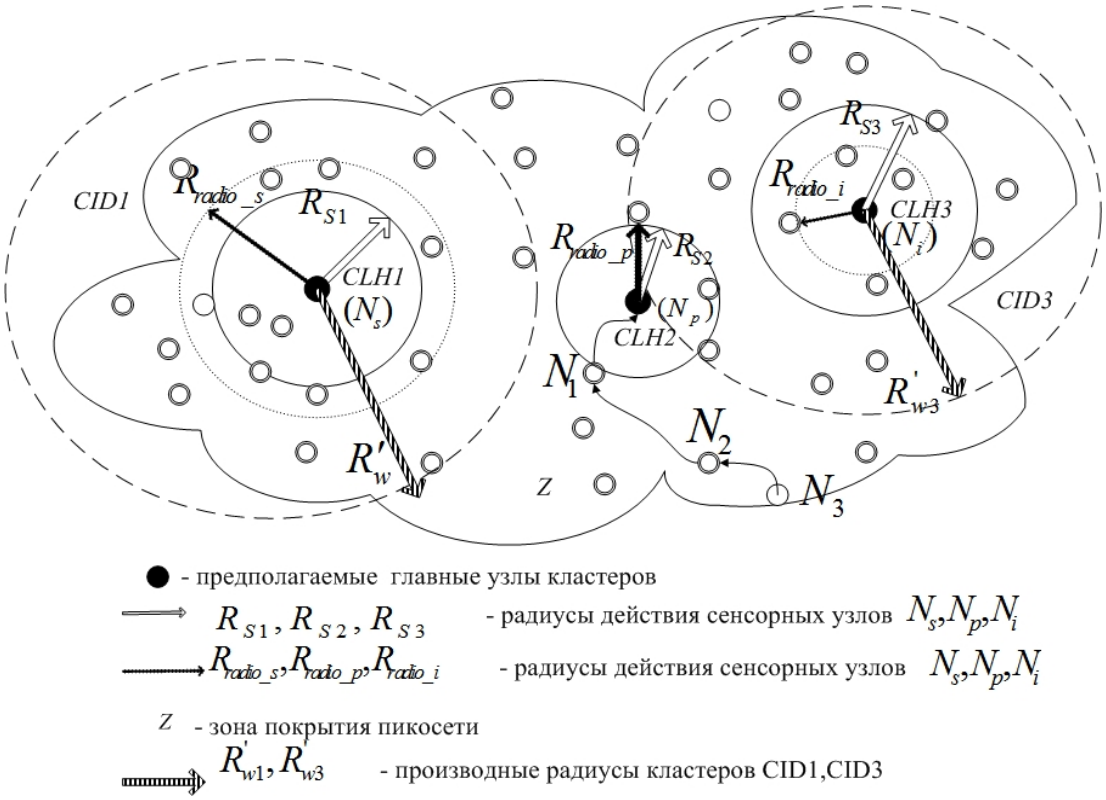


Рис. 2 - Процесс сбора данных в рамках зоны Z

Оптимальное положение агрегатора в пикосети определено на месте межкластерного шлюза. Такое положение позволяет агрегатору связаться минимум с двумя ГУК в рамках пикосети. Предложены подходы управления информационным потоком в кластерах, пикосетях и между ними. Такой подход применен в модели [5].

Разработанная модель БСС на основе пикосетей может быть применена для совместного использования ранее не совместимых алгоритмов управления информационными потоками в рамках одной сети.

Литература:

1. Галкін П.В. Аналіз моделей та оптимізації збору інформації в бездротових сенсорних мережах [Текст] / П. В. Галкін // Восточно-Европейский журнал передовых технологий.– 2014.– т.5, №9 (71).– С. 24-30.

2. Галкин П. В. Анализ энергопотребления узлов беспроводных сенсорных сетей //ScienceRise. – 2014. – №. 2 (2). – С. 55-61

3. Галкин П. В. Алгоритм управления и оптимизации информационных потоков в беспроводной сенсорной сети //Восточно-Европейский журнал передовых технологий. – 2014. – №. 6 (3). – С. 53-63.

4. Галкин, П. В. Модель сбора информации в беспроводной сенсорной сети / П. В. Галкин // Наукові записки Українського науково-дослідного інституту зв'язку. – 2014. – №5(33). – С. 41–53

5. Галкін П.В, Ключник І.І. Спосіб збору інформації в бездротовій сенсорній мережі : пат. на корисну модель 100463 Україна / Галкін П. В., Ключник І. І. ; ХНУРЕ. – 2015

ТЕХНОЛОГІЇ СЛАЙСІНГА У МЕРЕЖАХ 5G

Демченко І.В.
Науковий керівник – старший викладач Булашенко А. В.
Київський політехнічний інститут ім. Ігоря Сікорського, м. Київ, Україна
(03056, Київ, пр. Перемоги, 37, каф. теоретичних основ радіотехніки)
e-mail: an_bulashenko@i.ua, 095-702-99-09

This work is devoted to splicing methods in modern communication networks 5G. The network splicing capabilities of networks 5G / IMT-2020 are analyzed. The technology supports networks with Programmable Parameters (SDNs) and Virtualization of Network Functions (NFVs), representing the future of the communications industry, in which virtualized infrastructures and services provide network flexibility and network programming.

Майбутні мережі зв’язку 5G/IMT-202 повинні забезпечувати процес налаштування мережі за вимогами до конкретних послуг, наприклад встановлення необхідної швидкості передачі даних, затримки, надійності, безпеки та інших сервісів для різних категорій користувачів. Для цього в мобільних мережах 5G/IMT-2020 вводиться технологія слайсінга. Слайсінг – це можливість ізолювати і захищати шари з різними віртуальними мережами один від іншого. Технологія 5G надає не тільки мобільний зв'язок і доступ в Інтернет, але також роботу Інтернету речей, підключення до мережі передачі даних для збільшення безпеки автономних систем (наприклад, автопілотів автомобілів і дронів), банківський і промисловий Інтернет. З точки зору оператора мобільного зв’язку, слайсінг складається у створенні за запитом користувачів набору віртуальних мереж, що розміщені за загальною фізичною інфраструктурою, кожен з яких налаштований для надання специфічних послуг.

Мережевий слайсінг (рис. 1) може бути поданий як віртуальна мережа, що працює незалежно від її фізичної інфраструктурної мережі. Наприклад, віртуальний мережевий міст між віртуальним вузлом мережі та його фізичним вузлом. Віртуальний вузол мережі може виконувати спеціальний ряд мережевих послуг як звичайний фізичний мережевий вузол (маршрутизатор, брандмауер, або сервер мережевих послуг). Встановлення віртуальних мережевих мостів може бути здійснено SDN комутатором. Технологія SDN [1] дозволяє автоматично керувати віртуальною топологією мережі. Отже, можливість виділення необхідних ресурсів та зміна топології мережі є потрібний функціонал для утворення мережевого слайсінга. Віртуальний мережевий вузол може бути встановлений при використанні технологією NFV. Технології SDN та NFV дозволяють слайсінг в мережах зв’язку задовольняти вимогам високої степені гнучкості мережі.

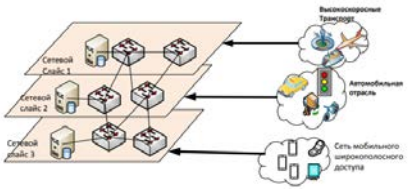


Рис. 1

Організація мереж з програмованими параметрами (SDN) та віртуалізація мережевих функцій (NFV) являють собою майбутнє індустрії зв'язку, в якій віртуалізовані інфраструктури та послуги забезпечують гнучкість та програмованість мережі. Архітектура мереж SDN підтримує принципи мережевого слайсінга оскільки SDN дозволяє керувати загальною інфраструктурною мережею та ефективно підтримувати декілька клієнтських зразків мережі.

Технологія слайсінга підтримує різноманітні можливості на загальній інфраструктурній мережевій платформі. Тому у мережах 5G/IMT-2020 необхідні нові та більш гнучкі підходи реалізації підтримки майбутніх інноваційних технологій. Мережевий слайсінг вже розглядається як провідний компонент для оптимального використання мережевих інфраструктур. Крім того, технологія дозволяє провайдерам мережевих послуг створювати та керувати групою захищених ресурсів. Роботи по тестуванню можливостей технології слайсінга в мережах 5G/IMT-2020 компанією SK Telecom та Ericsson продемонстрували можливості слайсінга у мобільних мережах 5G/IMT-2020. Різні споживачі Інтернету вимагають різного рівня якість доступу, швидкість доступу та рівень безпеки. Наприклад, дані з пристроїв, що підключені до Інтернету речей, можуть передаватися з істотно меншою швидкістю і не мати постійного з'єднання з Інтернетом. Для всіх перерахованих вище прикладів можуть бути використані різні частоти і різні "шари" каналів передачі даних, при цьому фізично буде використовуватися одна і та ж мережа. Таким чином, технологія слайсінга дозволяє більш ефективно (оптимізація за параметрами гроші, швидкість, надійність та час затримки) використовувати мережеві ресурси (копроративні, промислові мережі та інтернет речей).

Перелік посилань

1. Vladyko A. Comprehensive SDN Testing Based on Model Network / A. Vladyko, A. Muthanna, R. Kirichek // Lecture Notes in Computer Science. – 2016. – Vol. 9870. – p. 539–549.

2. Amerini I. Splicing forgeries localization through the use of first digit features / I. Amerini, R. Becarelli, R. Caldelli, A. Del Mastio // IEEE International Workshop on Information Forensics and Security (WIFS) – 2014. – p. 143-148.

3. Кучерявый А. Е. Самоорганизующиеся сети / А.Е. Кучерявый, А.В. Прокопьев, Е.А. Кучерявый. – СПб.: Любавич, 2011. – 312 с.

АНАЛІЗ РОБОТИ МЕТОДУ ІЄРАРХІЧНОЇ МІЖДОМЕННОЇ МАРШРУТИЗАЦІЇ

Жуга Ю.С.
Науковий керівник – к.т.н., асистент каф. ІКІ Невзорова О.С.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки,14, каф. Інфокомунікаційної інженерії,
тел. (057) 702-13-06)
e-mail: yurii.zhuha@nure.ua, телефон (097) 379-97-42

The main idea of the model is its decomposition representation and formulation the inter-area interworking conditions. The implementation of these conditions guaranteed the connectivity of calculated inter-area paths. The proposed method is based on goal coordination principle that guaranteed the coordination procedure convergence in finite number of iterations which was confirmed on a set of examples.

Ієрархічна побудова сучасних телекомунікаційних мереж (ТКМ) є адекватною реакцією на постійне зростання їх територіальної розподіленості, зростання числа комутаційних і термінальних пристроїв, розширення кількості наданих ТКМ інфокомунікаційних сервісів і ін. [1-2]. Основним недоліком вже реалізованих на практиці технологічних рішень те, що протоколи OSPF, IS-IS і PNNI переважно базуються лише на топологічній (структурній) ієрархії ТКМ, яка, не підкріплена ієрархією функціональною. Вихід із становища бачиться в переході до декомпозиційних потокових моделей, що дозволяють найбільш адекватно описати процеси ієрархічної маршрутизації в сучасних ТКМ.

Основу методу покладає потокова модель міждоменної маршрутизації, особливістю якої є її декомпозиційне представлення з формулюванням умов міждоменної взаємодії, виконання яких гарантувало зв'язність розрахунків міждоменних шляхів [1]. Також для формування метода ієрархічно-координаційної маршрутизації використовується принцип цільової координації. За рахунок використання якого вдалось корректно сформувати задачі ієрархічних рівнів: нижній відповідає за розрахунок вектора маршрутних змінних, а верхній рівень – за організацію міждоменної взаємодії, що гарантувало збіжність координуючої процедури за кінцеве число ітерацій, що було підтверджено на великої кількості розрахункових прикладів.

Було досліджено працездатність методу [1] на прикладі централізованої системи та тієї ж системи, але розподілену на три домени (рис. 1).

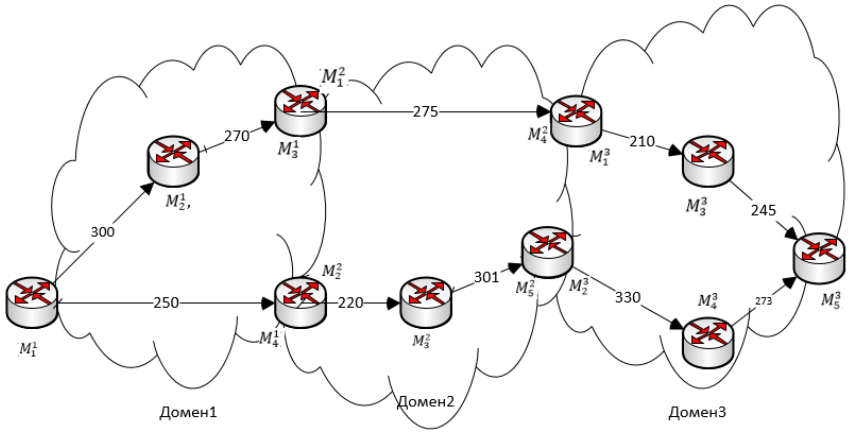


Рисунок 1 – Структура ТКМ, що містить декілька доменів

Дослідження методу було проведено середовищі MATLAB. В ході дослідження запропонованого методу ієрархічно-координаційної міждоменної маршрутизації було проаналізовано вплив структури мережі, зв'язності маршрутизаторів, числа прикордонних маршрутизаторів, і завантаженості ТКМ на збіжність координуючої процедури. Результати дослідження засвідчили, що на зростання числа ітерацій процедури впливали підвищення завантаженості ТКМ, якщо це супроводжувалося реалізацією багатоколійної стратегії маршрутизації, а також збільшення числа прикордонних маршрутизаторів. Це пояснювалося зростанням числа можливих варіантів вирішення завдань маршрутизації в окремих доменах, що і призводило до деякого збільшення числа координуючих ітерацій (до 3-4). Використання координуючої процедури дозволило наблизити якість розподіленої маршрутизації по доменах до результатів централізованої маршрутизації, але істотно знизивши при цьому розмірність розв'язуваної оптимізаційної задачі. Реалізація досліджуваної математичної декомпозиційної моделі і методу ієрархічно-координаційної міждоменной маршрутизації в телекомунікаційній мережі дозволить підвищити маштабованість маршрутних рішень за рахунок зниження обчислювальної складності розв'язуваних маршрутних завдань, а також зменшення обсягів службової інформації про стан мережі, що циркулює в ТКМ.

Перелік посилань:

1. Лемешко А.В., Невзорова Е.С., Арус К.М. Анализ сходимости координационной процедуры при реализации иерархической маршрутизации в телекоммуникационной сети [Електронний ресурс] // Проблеми телекомунікацій. 2015. № 1 (16). – С. 54-71.

2. Лемешко О.В.,Невзорова Е.С. Розробка і аналіз методу ієрархічних-координаційної міждоменної маршрутизації в телекомунікаційной мережі // Наукові записки УНДІЗ. – 2016. – № 4 (44). – С.42-68.

MEASUREMENT OF REFERENCE SIGNAL RECEIVED POWER IN LTE

Master student Z. A. Zulkarnain
Supervisor - PhD Kadatskaja O.
Kharkov National University of Radio Electronics
(61166, Kharkov, Nauka Avenue, 14, Info communication Engineering Department, tel. (057) 702-13-20),
E-Mail: tkc@kture.kharkov.ua fax (057) 702-13-20

In this work the reference signal received power (RSRP) is studied. It has been defined in a number of ways. Some of these definitions have been looked at including the 3GPP's definition. As an RSSI type of measurement, its relationship with RSSI is also established. The reporting range as well as a brief calculation of RSRP has also been done in this piece of work.

For 4G LTE, RSRP, RSRQ and SINR are the metrics measured by the User Equipment on reference signal (RS). Parameters RSRP and RSRQ are key measures of signal level and quality for modern LTE network. In this article, the focus is on the study of the RSRP measurement in LTE. RSRP is an RSSI type of measurement. Essentially, it measures only the reference power and does not give any information about the signal quality. It is the most important measurement that the UE has to do for cell selection, reselection and handover. This important parameter is studied and some practical work done.

Received Signal Strength Indicator (RSSI) is a measure of the average total received power observed of the carrier RSSI only in OFDM (Orthogonal Frequency Division Multiplexing) symbols containing reference symbols for antenna port 0 in the measurement bandwidth over N resource blocks. The carrier's RSSI total received power includes the power from co-channel serving and the non-serving cells, the adjacent channel interference, the thermal noise, among others.

It provides information about the total received wide-band power. All symbols are measured including all interference and thermal noise. UE do not report RSSI to eNodeB. RSSI is simply computed from RSRP and RSRQ which are reported by UE. From the above, it could be deduced that,

$$RSSI = ns + sc + inp,$$

where ns is noise
sc is serving cell power
inp is interference power

It implies that without noise and interference, there is 100% downlink (DL) physical resource block (PRB) activity. In this case, we can say that

$$RSSI = 12*N*RSRP,$$

where -RSRP is the received power of 1 resource element (1RE), that is average of the power levels received across all Reference Signal symbols within the considered measurement frequency bandwidth.

N -the number of resource blocks (RBs) across the RSSI.

RSRP- is the linear average of reference signal power (in Watts) measured over a specified bandwidth (in number of REs).

This is the most important measurement UE has to do for cell selection, re-selection and handover. It is very similar to CPICH RSCP in WCDMA. The average here is with respect to the received power of a single reference signal resource element. So, the power of multiple resource elements is measured by the UE and the average of which is taken. The resource elements are those used in the transfer of the reference signals.

According to the 3GPP definition in 36.214 specifications, RSRP is the linear average over the power contributions of the resource elements that carry cell-specific reference signals within the considered measurement frequency bandwidth. For RSRP determination the cell-specific reference signals R0 according to TS 36.211 shall be used.

This parameter measures only the reference power and does not give any information about the signal quality. Information about the signal strength of the desired signal is obtained. Usually the UE measures RSRP based on the direction (RRC message) from the eNodeB and report the value. A non-negative value ranging from 0-97 is send. Each of these values is mapped to specific range of values of real RSRP values as defined in 3GPP specifications 36.133.

The reporting range is between -44 to -140dBm. This is with 1dB resolution. This corresponds to the range of non-negative values from 0-97 that is sent by the UE. Measuring signal power while potentially excluding noise and interference is a unique characteristic of RSRP.

Consider a single antenna system. Let’s assume the Reference Signal Transmitted Power is about 20dBm and the path loss experienced by a UE located elsewhere in the cell is 100dB. Then by definition, the RSRP measured by the UE is 20 – 100 = -80dBm. Comparing this value to the table of real values of RSRP as in the 3GPP specification 36.133, it corresponds to RSRP integer value 60. In this case UE can report RSRP = 60 in the measurement report.

References

1. https://www.itu.int/rec/T-RECOMNDAITION -G.729

MEASUREMENT OF REFERENCE SIGNAL RECEIVED QUALITY IN LTE

Z. A. Zulkarnain
Supervisor - PhD Kadatskaja O.
Kharkov National University of Radio Electronics
(61166, Kharkov, Nauka Avenue, 14, Info communication Engineering Department, tel. (057) 702-13-20),
E-Mail: tkc@kture.kharkov.ua fax (057) 702-13-20

In this work the reference signal received quality (RSRQ) is studied. It has been defined in a number of ways. Some of these definitions have been looked at including the 3GPP's definition. The reporting range as well as a brief calculation of RSRQ has also been done in this piece of work.

In LTE network, there are two parameters measured by the UE (User Equipment) on reference signal (RS). These parameters are RSRP and RSRQ. These parameters are key measures of signal level and quality for modern LTE network. In this article, the focus is on the study of the RSRQ measurement in LTE. Unlike RSRP, RSRQ give information as to the quality of the reference signal. It is equally an important measurement that the UE has to do for a reliable cell selection, reselection and handover. This important parameter is studied and some practical work done.

RSRQ can be defined as the purity of Reference Signal (RS) across the system bandwidth. It is a calculated value from RSSI and RSRP. It simply denotes a measure of signal and interference. It indicates the quality of the received reference signal (RS). RSRQ measurement provides additional information when RSRP is not sufficient to make reliable handover or cell selection/re-selection decision. In handover procedure, the LTE specification provides the flexibility of using RSRP, RSRQ or both. When the RSRP is sufficient enough to provide a reliable handover, it used, if not then it is used alongside the RSRQ. Whichever case is applicable, must be measured over the same bandwidth. As in the case of RSRP, UE reports an integer value to eNodeB. The value ranges from 0-34. 3GPP has provided a table. Using the table, the integer value can be translated to a range of RSRP value in dB
Mathematically[1],

$$RSRQ = (N*RSRP)/RSSI,$$

where N - the number of resource blocks.

RSRP - Reference Signal Received Power

RSSI - Received Signal Strength Indicator

The 3GPP defined RSRQ [2] as the ratio of the product of the number (N) of the Physical Resource Blocks (PRBs) over which RSSI is measured and RSRP to E-UTRA Carrier RSSI. The measurements of the RSRP and the E-UTRA Carrier RSSI shall be made over the same set of resource blocks.
Mathematically,

$$\text{RSRQ} = \frac{Nprb * RSRP}{C\ RSSI},$$

where $Nprb$ is the number of Physical Resource Blocks

C RSSI is the E-UTRAN Carrier RSSI

It is worth noting that, the RSSI is the measurement of the pure wide band power, which includes noise, serving cell power and interference power during reference signal symbol. The reporting range of RSRQ is from -3 to -19.5dB.

For RSRQ to be maximum it is based on the assumption that RS REs are occupied, no traffic what so ever. There are two RS REs per OFDMA symbol. As such

RSRQ = $\frac{Nprb * RSRP}{C\ RSSI}$ = RSRP/ (2xRSRPx $Nprb$ / $Nprb$)

The maximum value of RSRQ is therefore = 0.5 = -3dB

The absolute accuracy for intra-frequency RSRQ is between +/-2.5 and +/-3.5dB. No relative accuracy is specified for intra-frequency case. The absolute accuracy for inter-frequency RSRQ is between +/-2.5 and +/-3.5dB. Finally, the relative accuracy between the inter-frequency and the intra-frequency is between +/-3dB and +/-4dB.

References

1. https://mauriziolarocca.com/78-rsrp-and-rsrq-measurement-in-lte/
2. https://www.itu.int/rec/T-RECOMNDAITION -G.729

ТАКТИЛЬНИЙ ІНТЕРНЕТ У МЕРЕЖАХ 5G

ЗіменкоД.О.
Науковий керівник – старший викладач Булашенко А. В.
Київський політехнічний інститут ім. Ігоря Сікорського, м. Київ, Україна
(03056, Київ, пр. Перемоги, 37, каф. теоретичних основ радіотехніки)
e-mail: an_bulashenko@i.ua, 095-702-99-09

The work describes the personality of the viticulation of tactile internet. Tactile Internetis a tactile feed back in teraction, the technical systems of which support not only audio and video interactions, but also the part of robotic systems that are managed as quickly as the user does not notice the delay time.

Дослідження тактильного інтернету активно ведуться по всьому світу [1-3]. Роботизована рука, роботизована рукавичка, які дають можливість відчути, «помацати», віртуальну реальність. Це все є основні розробки нової ери Тактильного Інтернету.

Технології як SCMA, F-OFDM та полярний код є розробкою компанії Huawei для реалізації так званого Тактильного Інтернету.

Певний набір параметрів буде використовуватися для кожної задачі, для цього організовано розбиття на підносійніплощини в модернізованій технології OFDM. Це все є F-OFDM (Filtered-OFDM).

Перші тестування показали, що завдяки використанню вільних захищених смуг в системі LTE(4G), технологія F-OFDM забезпечує збільшення загальної пропускної здатності всієї системи на 10 %.А також, ця технологія підтримує асинхронну передачу даних для рідних користувачів, завдяки чому, та сама пропускна здатність збільшується аж на 100% у порівнянні із системою для передачі трафіку LTE.

Більш широкий доступ для окремих пристроїв може забезпечити нам технологія багато-стаціонарного доступу, яка побудована на основі розрідження кодів, щодозволяє нам комбінування технології OFDMA з CDMA кодом. Ця не ортогональна технологія називається SCMA (SparseCodeMultiple Access). Вона була розроблена спеціально для можливого використання у мережах п’ятого покоління. Ідея цієї технології полягає в покращені спектральної ефективності безпровідного радіо доступу. Принципом роботи полягає у тому що, вхідний потік даних на пряму перетворюється в кодові слова, які складаються з символів різного типу шифрування. Кожне кодове слово являє собою один із розподілених рівнів передачі (transmissionlayer). Для кожного, конкретного рівня підбирається кодове слово з кодових книгSCMA. Завдяки чому, декілька потоків даних можуть розподілити одні й ті самі частотно-часові ресурси OFDMAсигналу. Більш гнучкийта ефективний адаптаційниймеханізм, підвищенняпропускноїздатності(для низхідного каналузв’язку на 80 %), зменшеннязатримки передачі,такожзбереження електроенергії,збільшує

кількістьпідключених пристроїв на 300%, це всі ті якості які надає нам технологіяSCMA.

Використання кодерів і декодерів послідовного анулювання дає можливість кодові досягти ємності каналу Шенона, і такий код називається PolarCode.Полярний код є однією із найзручніших технологій для кодування кодівз прямим виправленням помилок. На відмінно трубко коду, що використовується у так званому 4G(LTE), полярний код може забезпечити коефіцієнтом підсилення 0,5 - 2 дБ. 27 Гбіт/с – це є пікова швидкість, яка була досягнута за певних умов у низькоходномурежимі.

Компанією ZTE було запропоноване рішення множинного доступу, що дозволяє в мережах з високим навантаженням цей самий множинний доступ без необхідності планування мережі.Це рішення називається MUSA (Multi-UserShared Access). Дозволяє покращити покриття мережі, та значно збільшити кількість підключень пристроїв до системи. Упорівнянні із мережами попередніх покоління помітили збільшення пропускної здібності на 200 %, у ході досліджень. Також спостерігається збільшення граничного допустимого навантаження до трьох разів.

При реалізації концепції Тактильного Інтернетуу домашній мережі, новий стандарт IEEE 802.11ad працює в діапазоні частот 5 ГГци з максимальноюшвидкістю передачіданих 7 Гбіт/с.

Компанія Ciscозапропонувала DWDM платформу, для передачі великого об’єму даних на досить великі відстані.

Розділяючи час на малі інтервали так, що збільшується об’єм перенесених біт з декількох вхідних джерел, для передачівеликого об’єму даних на великівідстані компанія Технологія мультиплексування із розділенням по часу (TDM) збільшує пропускну здатність.

Таким чином, Тактильний Інтернет розглядається як однеіз ключових доданків в мережах 5G (IMT-2020). На сьогодні ведуться роботи подослідженню методів передачі тактильних відчуттів через мережуз використанням Інтернетаречей.

Перелік посилань

1.Meryem S. The 5G-Enabled TactileInternet: Applications, Requirements,andArchitecture /S.Meryem, A.Adnan, D.Misch// IEEE WirelessCommunicationsandNetworkingConference (WCNC). – 2016. – pp. 1–6

2.Martin M.TheTactileInternet: Vision, RecentProgress, andOpenChallenges/ M.Martin, C.Mahfuzulhoq, P.Bhaskar, P.Dung// IEEE CommunicationsMagazine. – 2016. –Vol. 54. – pp. 138–145.

3.Changyang S. EnergyEfficientDesignforTactileInternet/S.Changyang, Y.Chenyang// IEEE/CIC InternationalConferenceonCommunicationsinChina (ICCC). – 2016. – pp. 1–6.

МЕТОДИ КОНВЕРГЕНЦІЇ ПОСЛУГ МОБІЛЬНОГО ЗВ'ЯЗКУ НА ПЛАТФОРМІ IMS

Козубенко В.С.
Науковий керівник – доц. Сабурова С.О.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. інфокомунікаційної інженерії,
тел. 38 (099) 529-65-31), vitalii.kozubenko@nure.ua

IMS architecture is considered by many operators and service providers as well as equipment suppliers as a possible solution to the issues of further development of services and for the construction of next-generation networks, and as a basis for convergence of mobile and fixed networks on the IP platform.

Мобільний зв'язок – одна з найбільш стрімко розвивающих індустрій в сучасному світі. В даний час досить актуальним і досить складним є перехід до технологій мобільного зв'язку 3-4G, що забезпечує високоякісну передачу мови, зображень, послуги мультимедіа та доступ в Інтернет, а також безпосередній зв'язок мобільного телефону з комп'ютером.

Загальною стратегічною метою систем 3-4G є задоволення потреб масового споживача у послугах глобального персонального мультимедійного рухомого зв'язку. Загальна функціональна архітектура систем 3-4G містить три основних модулі:

Загальна мережа радіодоступу (IMS, підсистема IP-мультимедіа) для надання послуг абонентам 3-4G за допомогою стандартизованих радіоінтерфейсів. Загальна транспортна мережа (CN) для передачі магістрального трафіку і організації взаємодії (конвергенції) на основі мереж рухомого зв'язку 2-4-го поколінь. Користувальницькі додатки для надання мультимедійних послуг незалежно від технології радіодоступу.

Аналіз світового досвіду підтверджує доцільність побудови загальної транспортної мережі вітчизняної системи 3-4G на основі конвергенції та об'єднанням магістральних діючих мереж рухомого зв'язку 2-3го покоління з використанням протоколів ATM і IP.

Концепція IP Multimedia Subsystem (IMS) описує нову мережеву архітектуру, основним елементом якої є пакетна транспортна мережа, що підтримує всі технології доступу і забезпечує реалізацію великого числа інфокомунікаційних послуг. Її авторство належить міжнародному партнерству Third Generation Partnership Project (3GPP), що об'єднав European Telecommunications Standartization Institute (ETSI) і кілька національних організацій стандартизації.

IMS спочатку розроблялася для розвитку послуг та побудови мобільних мереж 3-4го поколінь на базі протоколу IP. Надалі Концепція була прийнята комітетом ETSI−TISPAN, зусилля якого були спрямовані на специфікацію протоколів і інтерфейсів, необхідних для підтримки і

реалізації широкого спектру послуг в стаціонарних мережах з використанням стека протоколів IP.

Причину виникнення концепції IMS саме в середовищі розробників стандартів для мобільних мереж можна пояснити наступним чином: оператори фіксованих мереж активно підтримують перехід від традиційних телефонних мереж до мереж загального користування(МзЗК), пов'язуючи з ними певні надії на скорочення операційних витрат і капітальних вкладень, а також на розвиток нових послуг, очікуючи, як наслідок, істотного підвищення доходів.

Основна технологічна ідея МзЗК – поділ транспортних процесів і процесів управління викликами і сеансами на базі елементів платформи Softswitch не була підтримана своєчасною розробкою відповідного набору стандартів. Це призвело до того, що основні мережні елементи МзЗК, часто виявляються несумісними між собою.

У мережах мобільних операторів, де одним з основних джерел доходів є роумінг, така несумісність виявляється куди більш значним недоліком, ніж у стаціонарних мережах. Саме це і визначило активність міжнародних організацій (в першу чергу ETSI і 3GPP), які почали розробку нових принципів побудови і стандартів мобільних мереж 3G, грунтуючись на багаторівневій архітектурі МзЗК.

По суті концепція IMS виникла в результаті еволюції мереж UMTS, коли область управління мультимедійними викликами і сеансами на базі протоколу SIP додали до архітектури мереж 3-4G. Серед основних властивостей архітектури IMS можна виділити наступні: багаторівневість – розділяє рівні транспорту, управління і додатків; незалежність від середовища доступу – дозволяє операторам і сервіс-провайдерам конвергировать фіксовані і мобільні мережі; підтримка мультимедійного персонального обміну інформацією в реальному часі (наприклад голос, відео-телефонія) і аналогічного обміну інформацією між людьми та комп'ютерами (наприклад ігри); повна інтеграція мультимедійних додатків реального і нереального часу (наприклад потокові додатки і чати); можливість взаємодії різних видів послуг; можливість підтримки декількох служб в одному сеансі або організації декількох одночасних синхронізованих сеансів.

Список використаних джерел

1. Багатоканальний електрозв’язок та телекомунікаційні технології (Ч.2) / Лемешко О.В., Лошаков В.А., Поповський В.В., Сабурова С.О., Епишкин С.О. – Х.: ТОВ «Компанія СМІТ», 2018р.р.. – 482 с.

2. 2. S. Saburova, E./Bondar, ,E.Popovska, PROSPECTS FOE SERVICE PLATFORM pre-IMS, Радиотехника: Всеукр. межвед. научн. техн. сб. – 2010. – № 163, 13-19.

МЕТОД ЗБАЛАНСОВАНОГО УПРАВЛІННЯ ЧЕРГАМИ ВІДПОВІДНО ДО КОНЦЕПЦІЇ TRAFFIC ENGINEERING QUEUE

Мокряк А.А.
Науковий керівник – асистент каф. ІКІ Лебеденко Т.М.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки,14, каф. Інфокомунікаційної інженерії,
тел. (057) 702-13-06)
e-mail: andrii.mokriak@nure.ua, телефон (099) 908-82-78

The given work is devoted to the solving of relevant scientific and technical problem that is related to the process of queuing optimization with consistent solution of Congestion Management and Congestion Avoidance tasks, packet flows processing to improve quality of service by developing mathematical models and methods.

Важливим завданням розвитку сучасних телекомунікаційних мереж є підвищення якості обслуговування (Quality of Service, QoS) зростаючої кількості запитів користувачів. Серед великої кількості засобів підвищення якості обслуговування важливе місце займають методи управління чергами, що дозволяють ефективно поліпшити такі показники QoS, як середня затримка пакетів, джитер, кількість відкинутих пакетів без істотних витрат на модернізацію існуючої інфраструктури мережі. У свою чергу, особливості та ефективність технологічних рішень в області обслуговування черг залежать від тих математичних моделей і методів, які в них закладені. Були проаналізовані відомі рішення в області управління чергами в телекомунікаційних мережах. Розглянуто їх переваги й недоліки. Особлива увага приділена оптимізації процесу управління чергами із забезпеченням узгодженості рішень щодо диференційованої обробки пакетів різних пріоритетів шляхом розробки нових математичних моделей і методів для підвищення якості обслуговування в телекомунікаційній мережі в цілому.У методі збалансованого управління чергами використовуються два рівня розрахунків. На першому рівні відбувається агрегація потоків в залежності від пріоритету потоків та черг. Для забезпечення справедливого обслуговування пакетів одного і того ж потоку кожен з пакетів доцільно обробляти в рамках однієї з черг. Таким чином, відповідно до фізики розв'язання задачі змінна є булевою, тобто:

(1)

Умова збереження потоку виглядає таким чином:

. (2)

Диференціація якості обслуговування забезпечується за рахунок того, що потоки з різними пріоритетами (вимогами до якості обслуговування) обробляються в різних чергах. За допомогою формули (3) відбувається оптимальний розподіл потоків між чергами з урахуванням пріоритетів черг та класів потоків:

$$f = \sum_i \sum_j \left(k_p^i - k_o^j\right)^2 \cdot x_{ij}. \quad (3)$$

На другому рівні задається порядок розподілу пропускної здатності між чергами та розв'язується оптимізаційна задача для визначення змінних α та b_j. Була введена умова запобігання перевантаження:

$$\sum_i a_i \cdot x_{ij} \le \alpha \cdot b_j. \quad (4)$$

де α – керуюча змінна, що додатково вводиться та характеризує верхній поріг завантаженості пропускної здатності, виділеної потокам різних класів обслуговування. У такому формулюванні оптимізаційна задача відноситься до класу задач нелінійного програмування, так як критерій оптимальності є нелінійним. Керуюча змінна мінімізується:

$$\min \alpha. \quad (5)$$

Якщо перевести умову (4) у лінійну форму, то це дозволить значно знизити обчислювальну складність практичної реалізації запропонованого методу. Щоб це зробити було записано наступним чином:

$$\frac{\sum_i a_i \cdot x_{ij}}{\alpha} \le b_j. \quad (6)$$

Для зручності розрахунків була введена α^*:

$$\alpha^* \cdot \sum_i a_i \cdot x_{ij} \le b_j. \quad (7)$$

де модифікована керуюча змінна (α^*) підпорядковується умовам:

$$\alpha^* = \frac{1}{\alpha}, \quad (8)$$

$$0 \le \alpha^* \le \infty. \quad (9)$$

З урахуванням оновленого запису нерівностей (7) в оптимізаційній задачі другого рівня в ролі критерію буде виступати умова вигляду:

$$\max \alpha^*. \quad (10)$$

Після цієї операції оптимізаційна задача стане лінійного виду, але цільова функція буде максимізуватися.Для перевірки адекватності запропонованого методу був проведений експеримент у програмі MatLab. За його допомогою було розраховано пропускну здатність для кожної з черг, а також метрики агрегування потоків. Виходячи з результатів було розроблено графічну модель розподілення потоків по чергам.

Перелік посилань:

1. Вегешна Ш. Качество обслуживания в сетях IP: Пер. с англ. М.: Вильямс, 2003. 386 с.

2. Лемешко А. В., Лебеденко Т.Н. Линейная модель оптимального управления очередями на интерфейсе маршрутизатора телекоммуникационной сети // International Journal "Information Content and Processing". - 2017. - Vol.4, No. 2. - PP. 171-181

ИСПОЛЬЗОВАНИЕ ФАЗОВЫХ ДАННЫХ ПРИ ГОЛОСОВОЙ АУТЕНТИФИКАЦИИ

Пастушенко В.Ю., Пастушенко Н.С.
Научный руководитель – к.т.н., проф. Пастушенко Н.С.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Науки,14, каф. Инфокоммуникационной инженерии,
тел.(057)702-13-20
e-mail: Mykola.pastushenko@nure.ua

The scientific task of improving the quality indicators of voice authentication systems is considered. At present, this problem is being solved by identifying user features in the range of amplitude-frequency characteristics of the voice signal being analyzed and by improving decision-making procedures. At the same time, it has long been known that a significant improvement in quality indicators is associated with an increase in the signal-to-noise ratio, the volume of data being processed, and the informative parameters of the voice signal being processed. The tasks associated with the accounting and assessing the influence of phase data of the user voice signal in the authentication system are discussed in the report.

Для защиты финансовых ресурсов и конфиденциальной информации широко применяются пин-коды, пароли, идентификационные карточки, с помощью которых производится аутентификация пользователя. Однако, эти средства защиты не отличаются совершенством, поскольку их можно потерять или подделать. Поэтому в настоящее время широко используется биометрическая аутентификация пользователя, которая является решением вышеперечисленных проблем. В последнее время в системах доступа предпочтение отдается динамическим (поведенческим) биометрическим признакам, и в первую очередь, голосовому сигналу.

Обусловлено это тем, что голосовым системам отдается предпочтение по критерию эффективность/стоимость. Кроме этого, голосовые системы аутентификации (ГСА) обладают и рядом дополнительных преимуществ, таких как, простота, удобство использования, сложность подделки, возможность удаленного использования по каналам связи, неограниченное оперативное увеличение парольных фраз, доступность применения современных достижений цифровой обработки данных.

К сожалению, качественные характеристики современных голосовых систем аутентификации уступают системам, которые базируются на использовании статических биометрических признаков. Поэтому кратко рассмотрим причины этого.

Как известно, числовые показатели качества таких систем могут быть существенно улучшены за счет увеличения: отношения сигнал/шум обрабатываемых данных; объема анализируемых материалов регистрации,

по которым принимается решение; максимального учета при принятии решения информационных параметров регистрируемых сигналов.

При реализации процедур цифровой обработки сигналов могут быть использованы различные информационные параметры: амплитуда, частота, фаза и поляризация. Современные ГСА используют для аутентификации пользователя амплитудную и частоту информацию его голосового сигнала. При этом основные исследования сосредоточены на поиске признаков пользователя в области амплитудно-частотных характеристик голосового сигнала, а также на усовершенствовании процедур принятия решения по оценкам полученных признаков.

В тоже время давно известно, что фазовая информация является более информативным параметром и, очевидно, использование фазовых данных голосового сигнала позволит существенно повысить качественные характеристики ГСА.

В докладе рассматривается задача формирования фазовой информации голосового сигнала пользователя и анализируются основные направления ее использования.

Для формирования фазовых данных голосового сигнала широко и плодотворно используется преобразование Гильберта, которое ориентировано на обработку гармонических стационарных временных рядов. В тоже время, голосовой сигнал - полигармонический нестационарный временной ряд.

Поэтому после формирования фазовых данных необходимо выполнить их предварительную обработку. Причины некорректного расчета фазы голосового сигнала следующие: область изменения функции arctg находиться в пределах от $-\frac{\pi}{2}$ до $\frac{\pi}{2}$, в тоже время фазовый угол изменяется от 0 до $2\cdot\pi$ (имеет форму пилообразного сигнала неизвестной длительности); имеют место ошибки в определении фазового угла, в том числе и аномальные, обусловленные ошибками в регистрации голосового сигнала и некорректной работой преобразования Гильберта.

Учет априорной информации о форме фазового сигнала позволяет откорректировать не только фазовые данные голосового сигнала, но и материалы регистрации, а также рассчитываемую квадратурную составляющую аналитического сигнала. Такая корректировка дает возможность уточнить оценки признаков пользователя как в области амплитудно-частотных, так и в области фазочастотных характеристик анализируемых данных. Последнее позволит существенно улучшить числовые показатели качества принимаемых решений по аутентификации пользователя.

На основе обработки экспериментальных данных показана обоснованность и достоверность предложенного пути усовершенствования голосовых систем аутентификации пользователя.

VOIP-BASED MULTIMEDIA SERVICE

Rami Tabaja
Supervisor - PhD Kadatskaja O.
Kharkov National University of Radio Electronics
(61166, Kharkov, Nauka Avenue, 14, Info communication Engineering Department, tel. (057) 702-13-20),
E-Mail: tkc@kture.kharkov.ua fax (057) 702-13-20

In this work, we report an assessment on VOLTE. End-to-End traffic analysis shown by defining the number of calls on the PSTN Public Switched Telecommunications Network side, you can also define the amount of bandwidth needed on the IP leg of the call.

VOLTE is a VoIP-based multimedia service, in which, voice calls and video conference services can be provided. The basic difference between VOLTE and VoIP over LTE is that VOLTE traffic is guaranteed with given QOS parameters and is delivered over dedicated bear which has the highest priority while VoIP traffic is delivered over default bearer which only preserves “best effort” QOS. With VOLTE, the end user can enjoy voice and LTE data speeds simultaneously on a single carrier. Since operators are currently relying on their 2G/3G CS networks for voice services, there is no way to offer voice and LTE data simultaneously without the use of dual-transceiver devices capable of simultaneously access to both 2G/3G network and LTE network . When deploying VOLTE, mobile network operators have to face many difficulties and challenges.

It is important to examine the challenges that VOLTE brings to LTE. For mobile operators, in order to ensure that VOLTE provides the same high level service that 2G/3G CS voice provides today, three following benchmarks have to be met: Call completion and call retention rates of 99% or better. Total end-to-end delay of less than 300MS

Voice quality that is as good as or better than 3G circuit switch voice .
IMS is designed for call session control not only for LTE, but other network technologies as well, including UMTS, CDMA2000 Wi-Fi and even wired networks .So there must be the combination of interworking VOLTE with traditional circuit- switched voice.

The above challenges can be divided into three categories as follows:
Challenges of Technology: Due to the fact that VOLTE is based on IMS there are many new protocols which are related to IMS such as IPv6, Sig Comp IP Sec and P-headers that make matters worse. The integration of the LTE protocol stack with the IMS control layer is to be taken care of and end-to-end IMS signaling must be tested over the LTE access network. In addition, implementation of mobility between the packet switched LTE and the circuit switched networks is also an issue.

Challenges of Implementation: The operators would look for temporary solutions before moving on to a full-fledged IMS architecture. Challenges of User satisfaction: Performance of the network for crucial real-time services needs to be tested with real- time audio and video quality measurement tools. Calculation the bandwidth needed on the WAN link.

End-to-End Traffic Analysis show by defining the number of calls on the PSTN Public Switched Telecommunications Network side, you can also define the amount of bandwidth needed on the IP leg of the call

Let's CDR has the following statistics K 36,000 minutes per day S 12,882.4 minutes per day C 28,235.3 minutes per day.

You are making the assumptions that can use the ERLANG B model for sizing your trunk groups to the PSTN want to have a Grade of Service GOS of P.01 on each of your trunk groups.

Computing the traffic load for the PSTN links at each node as follows: K= 102 BHT Busy hour traffic a telecommunications traffic measurement given in ERLANGS S = 36.5 BHT C = 80 BHT.

By using the ERLANG B formula you will experience a blocking rate of ~0.01139. Use a codec G.729 to use between POPs with following bandwidth: 26.4 kbps per call full rate with headers 11.2 kbps per call with VAD With Voice Activity Detection 9.6 kbps per call with CRTP. Compressed Real-Time Protocol (CRTP) 6.3 kbps per call with VAD and CRTP.

The bandwidth needed on the link between the K and the S is: Full Rate: = 2.534 Mbps VAD = 1.075 Mbps CRTP = 1.651 Mbps VAD/CRTP = 700.8 kbps

The band width needed on the link between the K and C is: Full Rate: = 1.9 Mbps VAD = 806.4 kbps CRTP = 1.238 MBP VAD/CRTP = 525.6 kbps Therefore , VAD and CRTP have a substantial impact on the bandwidth needed on the WAN link.

The evolution of operator infrastructure has led to the implementation of soft switches that allow migration to an All-IP network. However, the IMS architecture has been dominating industry due to its open interfaces for the deployment of converged services. The main challenge is to provide a consistent end-to-end Quality of Service through an IP service, such that the requested QOS requirements are satisfied when the deployment of a service involves the infrastructure of two or more operators, which are autonomous networks whose administrative domains are managed according to their own policies. Although operators must agree on the QOS requirements for a particular service among a set of IP services, operators do not configure their network devices in the same way because they have their own internal topology and QOS mechanisms that depend on their network devices and other non-technical management requirements.

ЗАБЕЗПЕЧЕННЯ ПОСЛУГ IoT 5G

Сушко Ю.В.
Науковий керівник - доц. Сабурова С.О.
Харківський національний університет радіоелектронікі
61166, Харків, пр. Науки, 14, каф. інфокомунікаційної інженерії,
тел. 0671503278, duginlambrozo36@gmail.com

The Internet of Things is a worldwide physical network in which all services can be connected and remotely controlled. As more and more devices are equipped with RFID or smart sensors, connecting "things" is becoming more simple. At the sensing level, wireless 5G smart systems with tags or sensors can now automatically be recognized and exchange information with various devices.

Інтернет у вигляді служб і контентів послуг, виникнувши в 1969 році, сьогодні міцно увійшов в наше життя. Пройшовши шлях від розробки протоколу TCP / IP, посилки першого електронного листа, появи системи доменних імен (DNS), запуску першого чату IRC, зародження Концепції всесвітньої павутини і протоколу HTTP, все прийшло до тієї колярової і зручною зображенні, яку ми бачимо зараз при відкритті браузера і навіть включення сучасного телефону.

І зараз технологія не стоїть на місці, проникаючи все далі і далі. Зараз, коли в світі править розвиток інформаційних технологій і передача даних, Інтернет проникає в звичні нам в повсякденному житті речі. І це явище неодмінно стає новою історичною віхою для Інтернет технологій.

Тому «Інтернет речей» можна розглядати в якості глобальної мережевої інфраструктури, що складається з безлічі підключених пристроїв, які використовують сенсорні, комунікаційні, мережні й інформаційні технології. Основною технологією для «Інтернету речей» є технологія RFID. За допомогою RFID-зчитувачів споживачи можуть ідентифікувати, відстежувати і контролювати будь-які об'єкти, автоматично підключені за допомогою RFID-міток. Технологія RFID широко використовується в логістиці, фармацевтичному виробництві, роздрібній торгівлі та управлінні ланцюгами поставок починаючи ще з 1980-х рр. Інша основна технологія для IoT - безпроводові сенсорні мережі (WSN), які в основному використовують взаємодіючі інтелектуальні датчики (сенсори) для спільної роботи і моніторингу. Область їх застосування включає в себе моніторинг навколишнього середовища, медичний моніторинг, виробничий контроль, моніторинг трафіку і т. д.

Досягнення в обох технологіях (RFID і WSN) внесли значний вклад в розвиток «Інтернету речей». Крім того, тепер безліч інших технологій і пристроїв, таких як штрих-коди, смартфони, соціальні мережі і хмарні обчислення, також використовується для формування широкої мережі підтримки IoT.

У зв'язку з розвитком безпроводового зв'язку, смартфонів і датчиків мережевих технологій все більше і більше мережевих «речей», або «розумних» об'єктів, беруть участь в IoT. В результаті всі ці IoT-технології роблять значний вплив на нові інформаційні та комунікаційні технології (ІКТ) і технології корпоративних систем.

Як ключова технологія інтеграції гетерогенних систем або пристроїв, Сервіс-орієнтована архітектура (SOA) для «Інтернету речей» може бути застосована для підтримки «Інтернету речей». SOA успішно використовується в таких науково-дослідних областях, як хмарні обчислення, безпроводові сенсорні мережі (WSN) і транспортні мережі. Чимало ідей було запропоновано для створення багаторівневих архітектур SOA для «Інтернету речей» відповідно до обраної технологією, потребами бізнесу і технічними вимогами. Наприклад, рекомендована Міжнародним телекомунікаційним союзом архітектура IoT складається з п'яти різних рівнів (або шарів): виявлення, доступ, підключення до мережі, проміжне ПО, шар додатків. Вчені запропонували розділити системну архітектуру IoT на три основних шару: рівень сприйняття, мережевий рівень і сервісний (або прикладної) рівень. Була розроблена для «Інтернету речей» тришарова модель архітектури, яка складається з прикладного рівня, мережевого рівня і шару зондування.

Архітектура «Інтернету речей» охоплює мережі і комунікації, «розумні» об'єкти, веб-сервіси і додатки, бізнес-моделі і відповідні процеси, спільну обробку даних, безпеку і т. Д. З точки зору технології при розробці архітектури «Інтернету речей» враховується можливість розширюваності, масштабованості, модульності і методи взаємодії гетерогенних пристроїв. Оскільки «речі» можуть пересуватися або потребувати у взаємодії з навколишнім середовищем в режимі реального часу, необхідна адаптивна архітектура.

Також децентралізована і гетерогенна природа «Інтернету речей» вимагає, щоб його архітектура надавала різні ефективні подієві можливості. Таким чином, SOA є хорошим методом для досягнення взаємодії різнорідних пристроїв безліччю різних шляхів.

Список використаних джерел

1. Ashton K. Internet of things. RFID J. 2. Van Kranenburg R. The Internet of Things: A Critique of Ambient Technology and the All-Seeing Network of RFID. The Netherlands, Amsterdam: Institute of Network Cultures, 2007. 3. Van Kranenburg R., Anzelmo E., Bassi A., Caprio D., Dodson S., Ratto M. The internet of things // Proc. 1st Berlin Symp. Internet Soc. Germany, Berlin, 2011.

УПРАВЛЕНИЕ УСЛУГАМИ LTE

Франсишко Сержиіо Бернардо
Науковий керівник – Сабурова С.О.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. Інфокомунікаційної інженерії,
тел. (057) 702-13-20) e-mail: lemur-97@mail.ru факс (057) 702-13-20

Service management as required by the QoS system provides end-to-end data transmission guarantees and is based on a system of rules for controlling LTE network performance tools, such as resource allocation, switching, routing, queue-serving mechanisms, and packet drop mechanisms.

В настоящее время общепризнанной основой для дальнейшего развития сетей связи общего пользования (ССОП) является концепция сетей связи следующего поколения - NGN (Next Generation Network), реализуемая на базе различных технических решений, прежде всего Softswitch [1-5] и IMS (IP Multimedia Subsystem). Как известно, концепция NGN предполагает создание сети связи с гарантированным уровнем качества обслуживания QoS (Quality of Service) пользователей, что достигается путем создания новых механизмов управления качеством обслуживания и установления определенных взаимоотношений между операторами связи, а также между оператором связи и пользователем на основе заключаемых соглашений об уровне обслуживания - SLA (Service Level Agreement). В соответствии с ITU-TY.1291 для обеспечения гарантированного уровня качества обслуживания в сетях NGN в качестве базового рекомендован алгоритм дифференцированных услуг (DiffServ).

С ростом разнообразия и сложности сервисов, предоставляемых в сетях NGN, оператор уже не может ограничиться просто контролем возможности передачи трафика и должен поддерживать на надлежащем уровне качество передачи. Решение этой проблемы обеспечивают OSS-системы, осуществляющие управление на основе мониторинга уровня обслуживания заказчиков (SLA-мониторинг).

Управление услугами на основе мониторинга различных приложений в единой, безопасной, проверенной и протестированной LTE сети позволяет корпоративным заказчикам эффективно и с высоким качеством использовать одну линию радидоступа для телефонии и видеоконференций, работы с приложениями корпоративных информационных систем типа клиент – сервер, электронной почты и работы с вебсерверами Интернет- контента. Обратная сторона интеграции – высокая зависимость бизнеса заказчика от обеспечиваемой оператором транспортировки трафика между пользователями. Более того, на практике возникают ситуации, когда, несмотря на имеющуюся возможность передавать трафик (т.е. доступность услуги), пользователь не может использовать то или иное приложение из-за низкого качества передачи

трафика оператором. В таких случаях принято говорить о деградации предоставляемого оператором сервиса.

Соответственно, в требованиях заказчиков к услугам оператора связи все чаще на первое место выходит не просто передача разнородного трафика, а предоставление сервиса нужного качества. И оператору требуются механизмы, позволяющие обеспечивать качество передачи трафика, отслеживать его уровень и представлять результаты своей работы заказчикам.

С точки зрения заказчика идеальным было бы просто перечислить в соглашении об уровне обслуживания (SLA) приложения, работоспособность которых гарантируется оператором. Однако для оператора, который обеспечивает всего лишь транспортировку трафика, такая постановка вопроса зачастую неприемлема – не все составляющие, влияющие на работоспособность приложения, находятся в зоне его ответственности. Исследуем показатели качества, которые могут быть включены в SLA и понятны как оператору (с точки зрения измерения), так и заказчику (с точки зрения их управления приложениями).

Особенности управления услугами LTE сети по обеспечению QoS и SLA следующие:

- Пакетная передача данных. Она позволяет сократить время за счет того, что заявка, поступающая на обслуживание, становится в очередь. Это занимает меньше времени, чем осуществление повторного запроса услуги. Кроме того, пакетизированный голос расходует полосу пропускания гораздо экономнее при молчании абонентов информация не передается.
- Физическое и логическое отделение передачи и маршрутизации пакетов от устройств и логики управления услугами позволяет использовать единый центр обработки вызовов для сетей разных типов (традиционных, пакетных, гибридных) с разными форматами речевых пакетов и с разным физическим транспортом, а также дает возможность повысить степень управляемости процессами и параметрами QoSв сетях.
- Функции качества обслуживания (QoS) заключаются в обеспечении гарантированного и дифференцированного обслуживания сетевого трафика благодаря передаче оператору контроля за использованием ресурсов и загруженностью сети. QoS представляет собой набор требований, предъявляемых к ресурсам сети при транспортировке потока данных.

В технологии LTE соглашения об уровне обслуживания - SLA должны также включать задержки, связанные с гарантий для установления цен классов обслуживания в зависимости от качества и пользовательской активности.

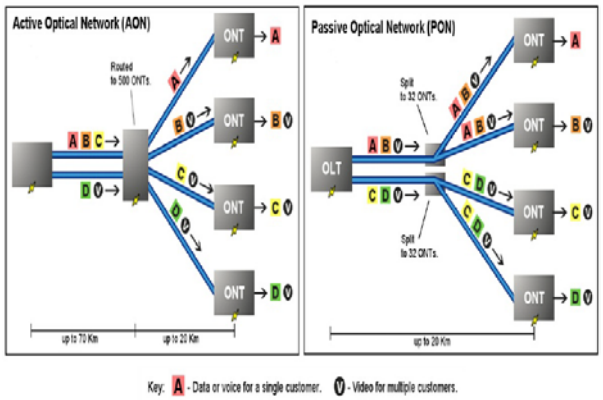
ВИКОРИСТАННЯ ТЕХНОЛОГІЇ PON В КОНЦЕПЦІЇ ІНТЕРНЕТ РЕЧЕЙ

Цилюрик В.Е.
Науковий керівник – ст.викладач, Ковальчук В.К.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки,14, каф. інфокомунікаційної інженерії,
тел. (057) 702-13-20)
e-mail: vadym.tsyliuryk@nure.ua

This paper is devoted to modern developments in the field of fiber-optic transmission lines used for systems of home devices that can perform actions and solve certain everyday tasks without human intervention. With the growing number of devices that are connected and controlled through the global network, the need for increased bandwidth for the Internet of Things is growing. In this paper, PON technology is considered as economically viable and satisfying all the needs of a smart home.

З розвитком Інтернету речей (Інтернет речей - це система, що об’єднує реальні речі у віртуальну мережу) кількість підключень до мереж абонентського доступу збільшується в рази. За прогнозами аналітиків, до 2021 року загальна кількість підключених пристроїв в світі складе 28 млрд. З них 1,5 млрд складуть споживча електроніка і розумні автомобілі, які взаємодіють один з одним. Останнім часом з`явилася концепція “Розумного буднку” (розумний будинок - сукупність простору і приладів в будинку, пов'язаних разом однією мережею) можна вважати частиною технології Інтернет речей.

Аналіз показує, що для Інтернету речей доцільно і економічно використовувати технологію PON – (Passive Optical Network – пасивна оптична мережа) – це найбільш перспективна технологія широкосмугового мультисервісного множинного доступу з оптичного волокна, що використовує хвилевий поділ трактів прийому/передачі, без використання активних мережевих елементів в вузлах розгалуження (рис.1).



OLT - optical line terminal; ONT - optical network terminal

Рис.1 Принцип дії PON

Це дозволяє багаторазово збільшити пропускну здатність, використовуючи всього один приймально-передавальний модуль в OLT для передачі інформації великій кількості абонентських пристроїв ONT і прийому інформації від них.

Головні переваги обраної технології - це економне використання волокна і невелика вартість абонентських терміналів, всі системи працюють на одному волокні, поділ обміну інформаційних потоків виконується на основі WDM-технології, тобто на принципі хвильового розподілу.

З урахуванням зростання пристроїв розумного будинку, які обмінюються даними в режимі реального часу, збільшується навантаження на мережу і час відгуку пристроїв. Так як швидкість світла в волокні становить $2 \cdot 10^5$ км/с та в лінії зв'язку активне обладнання використовується в меншій кількості, то час затримки зменшується.

В технології PON відстані OLT-ONT на 1 км буде відповідати збільшення часу затримки на подвійному пробігу на 0,01 мс.

$$T = L \cdot 0{,}01 \text{ мс}$$

Користувачеві доступно все одночасно і в повному обсязі: віддалений доступ до системи управління розумним будинком, моніторинг стану камер відеоспостереження, охоронна сигналізація, потоки даних, доступність всіх пристроїв, службові додатки, які цілком незалежні, ізольовані і захищені як в межах терміналу, так і в масштабі всієї проектованої мережі.

В основі ініціалізації мережі PON лежать три процедури:

- визначення відстаней від OLT до різних ONT ;
- синхронізація всіх ONT;
- визначення під час прийому на OLT потужностей оптичних сигналів від різних ONT.

Важливим моментом в технологіях PON є визначення черговості підключення абонентів до мережі. Черговість підключення абонентів досягається визначенням відстані OLT-ONT та часової затримки на цих ділянках. Ця процедура зветься ранжуванням абонентів за відстанню. В роботі розроблений алгоритм ранжування за відстанню.

Література

1. Гаскевич Е. PON – широкополосная мультисервисная сеть доступа:учеб./Е.Гаскевич, Р.Убайдуллаев.-К.: ТелеМультиМедиа, №2(12),2002, с. 29–32.

2. Башлы П.Н. Гигабит PON:пер.с англ.-К.: К.Гарстид GPON,Switzerland, Oct.21–31, 2003.

3. Ю. Королев УМНЫЙ ДОМ: приятная неизбежность:учеб./Ю. Королев, 2002, с. 12–22.

ДОСЛІДЖЕННЯ ХАРАКТЕРИСТИК СИСТЕМИ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ ПО РАЙДУЖНІЙ ОБОЛОНЦІ ОКА

Чернікова В.Г. Стрілець А.М.
Науковий керівник – к.т.н., доцент Астраханцев А.А.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки,14, каф. Інфокомунікаційної інженерії,
тел. (057) 702-55-92)
E-mail: valeriia.chernikova@nure.ua

This work is devoted to the actual problem of choosing a method for remote biometric authentication of an individual based on the Gabor filter and a combination of Gaussian and Laplace filters. The effectiveness of using the Gabor filter and the combination of Gaussian and Laplace filters was also investigated under the conditions of a combination of the above-mentioned with the same methods of processing the iris image from the CASIA-Iris-Interval database. The scientific novelty of the work is to further improve the methods of remote authentication of the individual by the iris and to investigate the effectiveness of using methods against background noise.

У зв’язку з швидкою еволюцією загроз традиційний захист інформації за допомогою паролю вже не є досить надійним. Йому на зміну приходять біометричні системи, деякі з яких за останні роки придбали досить велику популярність серед користувачів завдяки своїй захищеності та зручності використання. Серед таких систем, як найбільш стійку до підробки та безпечну для здоров’я можна виділити систему автентифікації по райдужній оболонці ока. Завдяки складності малюнку райдужної оболонки можливо відібрати близько 250 точок за допомогою яких забезпечується високий ступінь надійності автентифікації. На сьогодні не має єдиного стандартизованого алгоритму розпізнавання по райдужній оболонці, тому питання вибору найбільш оптимального є достатньо актуальним.

Зараз розпізнавання по райдужній оболонці поступається за популярністю лише методу автентифікації за відбитком пальцю і має гарні перспективи використання для посвідчення особи у біометричних паспортах та інших документах. На даний момент впроваджуються системи віддаленої біометричної ідентифікації у «хмарі» та на деяких сайтах державних послуг.

Процес розпізнавання по райдужній оболонці ока поєднує в собі декілька етапів: обробку зображення ока, застосування фільтру, генерацію коду райдужної оболонки на основі фільтру, занесення в базу та порівняння кодів райдужки з еталоном. Оскільки порівнюються не зображення, а коди, то механізмом, що забезпечує надійність системи, є застосування фільтру. У роботі досліджується ефективність двох механізмів – фільтру Габора та комбінації фільтрів Гауса та Лапласа – у поєднанні з іншими етапами розпізнавання по райдужній оболонці та

результати їх тестувань. Для перевірки ефективності та стійкості алгоритмів з різними фільтрами було виконано накладання шуму Перліна на тестові зображення. Для аналізу рівня завад, що був внесений пороговим значенням шуму для кожного із зображень, було підраховано значення «сигнал/шум». В результаті розрахунків було виявлено досить велике значення SNR для більшості зображень, що характеризує низьку кількість завад на зображеннях, що були зашумлені. На основі цього можна зробити висновок, що обидва фільтри є чутливими до накладання шуму, що свідчить про їх стійкість.

Для оцінки ймовірності виникнення помилок при роботі алгоритмів розраховуються показники FAR (False Acceptance Rate – коефіцієнт помилкового пропуску) та FRR (False Rejection Rate – коефіцієнт помилкової відмови в доступі).

Зашумлення зображення може призводити до неспрацьовуванні сканера (FRR), а не до прийняття зображення за інше з бази (FAR), оскільки мінімальні значення відмінностей (MSE) між оригінальними зображеннями складають 7,766, а максимальне значення MSE при впливі шумів при використанні фільтру Габора досягає 2,03. Враховуючи максимальне значення MSE при впливі шумів при використанні фільтру Габора було визначено, що майже 90% зображень мають ймовірність FAR близьку до нуля. Також була підрахована кількість зображень різних очей, MSE яких має менш ніж десятикратну відмінність від порогу шуму. В результаті цього було визначено FRR всіх досліджуваних зображень. Воно дорівнює 0,295 при використанні фільтру Габора та 0,047 при використанні комбінації фільтрів Гауса та Лапласа. Таким чином, показники ймовірності виникнення помилок свідчать, що використання в алгоритмі фільтрів Гауса та Лапласа є більш ефективним та безпечним. Результати досліджень можуть бути використані при побудові дистанційних систем автентифікації з передачею шаблону по відкритому каналу зв’язку з завадами. Практична значущість роботи полягає в можливості використання досліджуваних методів в системах біометричної автентифікації осіб із застосуванням мобільних пристроїв та передачею інформації по відкритих каналах зв’язку з завадами.

Перелік посилань:

1. Конахович Г.Ф. Цифрова стеганографія / Г.Ф. Конахович, А.Ю.Пузиренко. – К.: МК-Пресс, 2006, 40 с.

2. Колешко В.М. Традиційні методи біометричної аутентифікації і ідентифікації / В.М. Колешко, Е. А. Воробей, П. М. Азізов. – М. : БНТУ, 2009, 107 с.

МОДЕЛЬ СОСТОЯНИЯ И НАБЛЮДЕНИЯ ЭЛЕКТРОМАГНИТНОЙ ОБСТАНОВКИ В СЕТЯХ МОБИЛЬНОЙ СВЯЗИ

Н. А. Чурсанов
Научный руководитель – д.т.н., проф. Коляденко Ю.Ю.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Науки,14, каф. Инфокоммуникационной инженерии, тел. (057) 702-13-20)
e-mail: mykyta.chursanov@nure.ua факс (057) 702-13-20

A number of distinctive features that characterize the electromagnetic environment in mobile communication networks are highlighted: the multiple random natures of inter-element interactions; the network topology is characterized by a pronounced dynamics and non-stationarity, etc. It is concluded that the ratio of the power of the useful signal to the power of interference at a particular point in space is a random process. A model of the electromagnetic environment in mobile networks in the form of the equation of state and the equation of observation is proposed.

Элементы сетей мобильной связи (СМС) создают помехи для других элементов сети, которые в свою очередь являются объектами помеховых воздействий [1]. Разработано много методов, методик, теоретических обоснований посвященных улучшению электромагнитной обстановки (ЭМО) в радиолиниях, проблеме обеспечения электромагнитной совместимости (ЭМС) [2]. Ситуацию и саму ЭМО в СМС сильно усложняет тот факт, что в эту обстановку вносятся различные часто случайные факторы, носящие трудно прогнозируемый характер. В этих условиях рассчитать заранее ЭМО и решить задачу ЭМС с достаточной точностью не всегда удается, а часто просто невозможно из-за априорной неопределенности [1].

Можно выделить ряд отличительных особенностей, характеризующих ЭМО в СМС: множественный случайный характер межэлементных взаимодействий; топология сети характеризуется явно выраженной динамикой и нестационарностью и др.

Все это позволяет сделать вывод о том, что отношение мощности полезного сигнала к мощности помех $h = 10\lg\frac{P_c}{P_n}$ в конкретной точке пространства является случайным процессом, который представим уравнением состояния [3]:

$$\frac{d\vec{h}(t)}{dt} = F(t)\vec{h}(t) + G(t)\vec{\xi}(t), \qquad (1)$$

где $\vec{h}(t)$ - вектор состояния, который зависит от времени; $F(t), G(t)$ матрицы (для одномерного случая коэффициенты) состояния и возбуждения соответственно; $\vec{\xi}(t)$ – порождающее векторное белое гауссовское поле с нулевым средним.

Для стационарного случая коэффициенты F, G не зависят от времени. Коэффициенты F имеют физический смысл величин, обратных интервалу корреляции $\tau_{кор}$ процесса $h(t)$. Для одномерного случая:

$$F = -\alpha = -\frac{1}{\tau_{кор}}.$$

Коэффициенты G определяют масштаб случайных изменений процесса $h(t)$.

$$G = \sqrt{2\alpha\sigma^2},$$

где $\alpha = 1/\tau_{кор}$, σ^2 - спектральная плотность мощности порождающего процесса $\xi(t)$.

Для стационарного одномерного процесса $h(t)$ уравнение (1) представляется в виде:

$$\frac{dh(t)}{dt} = -\alpha h(t) + \sqrt{2\alpha\sigma^2} \cdot \xi(t). \qquad (2)$$

Алгоритм (2) обычно дополняется уравнением наблюдения. Модель наблюдения задается линейным алгебраическим соотношением:

$$y(t) = H(t)h(t) + n(t) \qquad (4)$$

где $H(t)$ - матрица, которая задает ослабление процесса; шум наблюдения $n(t)$ является белым гауссовский шумом с дисперсией D_n и нулевым средним.

Список использованных источников:

1. Поповский В.В. Методика анализа электромагнитной совместимости радиоэлектронных средств в группировках систем подвижной связи /В.В. Поповский, Ю.Ю. Коляденко/ Міжнародна науково-практична конференція «Актуальні питання регулювання у сфері телекомунікацій та користування радіочастотним ресурсом».- Київ 18-20 травня 2010 р. с. 115-116.

2. Теория и методы электромагнитной совместимости радиоэлектронных средств / Под редакцией Ю.А. Феоктистова.- М.: Радио и связь, 1988. – 216 с.

3. Вентцель Е.С., Овчаров Л.А. Теория случайных процессов и ее инженерные приложения/ Е.С. Вентцель, Л.А. Овчаров / / – М.: Наука. Гл. ред. физ. мат. лит., 1991. - 384 с.

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

AMAZON ALEXA VOICE ASSISTANT ON THE BASE OF RASPBERRY PI AS EFFECTIVE INSTRUMENT FOR COMMUNICATION

Akintunde Adedamola Emmanuel
Scientific supervisor- Ass Prof Maryna Yevdokymenko
Kharkiv National University of Radio-Electronics
Info communication engineering department
Nauki Ave Kharkiv, Ukraine.
Tel (063) 486 -99-31 email -akintundepelumi@yahoo.com

This paper describes and analyzes the development of Amazon Alexa voice assistant based on Raspberry Pi single-board computer. Also it describes the design of the voice assistant system, its system architecture with the hardware and software description which is required to keep the voice assistant up and running. As result in this paper will explained the implementation and testing of the voice assistant system working through its installation, launching, management and testing of the voice assistant system.

The main purpose of this paper is to implement a reliable voice assistant on mini embedded computer system. Voice assistants are very effective ways to organize our schedules. Almost all large technology companies have developed their own voice assistant – Amazon (Alexa), Google, and Apple (Siri) all developed ways to interface voice technology with so-called “Smart Homes”. For example, Amazon Alexa is a home speaker and “virtual assistant” personified by its call-name “Alexa.” It responds to voice commands to perform a wide range of functions such as playing music, providing news and weather updates, managing daily reminders and alerts, and working with a host of other subscription-based services and “smart home” devices.

For implementation of own voice assistant will based on an embedded system and Raspberry Pi. An embedded system is a computer system with a dedicated function within a larger mechanical or electrical system, often with real-time computing constraints. Embedded systems range from portable devices such as digital watches and MP3 players, to large stationary installations like traffic lights, factory controllers, and largely complex systems like hybrid vehicles, MRI, and avionics. Complexity varies from low, with a single microcontroller chip, to very high with multiple units, peripherals and networks mounted inside a large chassis or enclosure.

The Raspberry Pi is a series of small single-board computers developed in the United Kingdom by the Raspberry Pi Foundation to promote the teaching of basic computer science in schools and in developing countries.

The installation of the Amazon Alexa on the raspberry will start from installing raspbian OS on the SD card and connecting necessary hardware as follows. Hardware required: Raspberry Pi, Power adapter, HDMI cable, LAN cable, SD card and reader, Wireless keyboard and mouse, a computer to run the

installer (Etcher was used as the installer). Raspberry is then connected to a computer via Virtual Network Computing (VNC) viewer. VNC is a graphical desktop sharing system that uses the Remote Framebuffer protocol (RFB) to remotely control another computer. Before launching of the Amazon Alexa voice assistant based on Raspberry Pi single-board computer,we need to create our own Amazon developer account and create a profile for our DIY echo. We create a new profile and a security profile name. After setting up our profile, we setup the web settings since our device works with the internet..When we're done with the profile and web settings on AVS, we set up the terminal on our raspberry Pi. We update our device and install the scripts that will get Echo up and running.After succesful setup and log in alexa will automatically start up itself.

Afer the full installation of the echo on raspberry Pi, we put it to test. To be sure it was working appropriately.We logged in to the AVS for the account we created earlier on and it looks blank I the beginning, but once we start conversing with Alexa we see the questions asked abd the answers in the screen just to confirm it's working perfectly.

The advantages of designing our own voice assistant system on raspberry Pi is

- Raspberry can be used as a mini computer alongside the voice assistant.
- It is less expensive compared to the real voice assistant.

The disadvantages of designing our own voice assistant system on raspberry Pi is

- There are limitations to what Alexa can do.
- It doesn't support the alexa-to-alexa calling like the echo devices.
- And some of the features are locked in this region.(Traffic reports).

Overall, Voice assistant system was perfectly designed and implemented, and then it has been tested for unknown users.

List of references

[1] W. W. Gibbs, "Build your own Amazon Echo - Turn a PI into a voice controlled gadget [Resources_Hands on]," in *IEEE Spectrum*, vol. 54, no. 5, pp. 20-21, May 2017.

[2] P. Koopman, "Embedded system security," in *Computer*, vol. 37, no. 7, pp. 95-97, July 2004

[3] S. Jain, A. Vaibhav and L. Goyal, "Raspberry Pi based interactive home automation system through E-mail," *2014 International Conference on Reliability Optimization and Information Technology (ICROIT)*, Faridabad, 2014, pp. 277-280

ШЛЯХИ ЗАБЕЗПЕЧЕННЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ ПРИ ВИКОРИСТАННІ LINUX-ПОДІБНИХ СЕРВЕРНИХ ОПЕРАЦІЙНИХ СИСТЕМ

Добринін К.І.
Науковий керівник – к.т.н., доц. Добринін І.С.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки,14, каф. Інфокомунікаційної інженерії,
тел. (057) 702-13-20)
e-mail: kyrylo.dobrynin@nure.ua

The report is devoted to the problem of security of Linux servers when used in the enterprise on the example of a web server or a virtual server. The report shows the main attacks on Linux servers and the main ways to increase security on the server.

На сьогоднішній день значна кількість серверів працюють під операційною системою (ОС) Linux, яка поширюється під вільною і безкоштовною ліцензією. Абсолютна більшість спеціалізованих комп'ютерів, таких як веб-сервер, поштовий сервер, сервер баз даних або файл-сервер, працюють під ОС Linux. Основне завдання сервера полягає у виконанні сервісних функцій за запитом клієнта, надаючи йому доступ до певних ресурсів.

Для коректної роботи серверу актуальним є питання безпеки, тому що ОС Linux і пов'язані з нею сервіси сприйнятливі до спільних загроз, таким як: атака з метою заволодіти чужими даними, виведення серверу з робочого стану, отримання повного доступу до системи, тощо. Тому слід розглянути методи забезпечення безпеки сервера, що має важливе значення для захисту інформації на підприємстві.

У доповіді наведено рекомендації щодо забезпечення інформаційної безпеки і підвищення відмовостійкості Linux-сервера, не залежно від дистрибутива. Для злагодженої і коректної роботи сервера рекомендується подбати про безпеку системи ще на початковій стадії впровадження: встановити пароль на BIOS / UEFI, використовувати шифрування диску, встановлення надійного пароля для root-доступу.

Показано, що для підвищення захищеності системи доцільно виконати наступні рекомендації:

1. Своєчасно виконувати оновлення безпеки, які часто знаходять і виправляють критичні уразливості;
2. Не використовувати root-доступ для виконання неадміністративних команд;
3. Створити користувача з обмеженими правами і делегувати йому права суперкористувача (додаванням в групу sudo) для виконання повсякденних завдань, для яких не потрібні root-повноваження, від імені цього користувача;

4. Вимикати непотрібні сервіси. Деякі фонові процеси встановлені на автозавантаження і працюють до відключення системи, що може нести в собі певну небезпеку;

5. Використовувати двофакторну аутентифікацію з надійними ключами для доступу до сервера через SSH-з'єднання;

6. Змінити порт для SSH-з'єднання, що встановлений за замовчуванням, на будь-який інший;

7. Налаштувати права доступу для користувачів і впровадити регулярні зміни паролів;

8. Встановити вимогу складних паролів і блокування облікового запису після кількох невдалих спроб введення пароля;

9. Встановити і налаштувати міжмережний екран за допомогою вбудованого в ОС Linux контролера iptables;

10. Виконувати регулярне резервне копіювання на окремий диск, розділ або в безпечне віддалене сховище;

11. Використовувати систему моніторингу IDS/IPS (Snort, Suricata, Bro, Kismet);

12. Регулярно переглядати системні log-файли аудиту операційної системи, щоб своєчасно дізнаватися про помилки, а також про уразливості, з якими зіткнулися інші користувачі;

13. Використовувати один сервер для одного основного сервісу (ролі сервера);

14. Обґрунтовано використовувати різноманітні програмні продукти, наприклад: Linux-ACLs, LIDS (Linux Intrusion Detection / Defense System), AIDE (Advanced Intrusion Detection Environment) та інш.

Таким чином, використання перерахованих вище рекомендацій може призвести до збільшення захищеності інформації при використанні Linux-подібних серверних операційних систем.

Список використаних джерел:

1. Як захистити Linux-систему. [Електронний ресурс] - Режим доступу: https://habr.com/ru/company/1cloud/blog/309696/

2. Захист системи Linux: 11 порад з безпеки. [Електронний ресурс] - Режим доступу: https://proglib.io/p/linux-security/

3. Як захистити віртуальний сервер. [Електронний ресурс] - Режим доступу: https://vps.ua/wiki/install-linux-vps/security/

DEVELOPING A CONFERENCE APPLICATION FOR EDUCATIONAL PURPOSES WITH THE HELP OF CLOUD TECHNOLOGY

Ikwuegbu Chigozie Charles
Scientific supervisor – Ass. Prof. Maryna Yevdokymenko.
Kharkiv National University of Radio Electronics
Infocommunication engineering Department, Nauki Ave., Kharkiv
Tel. (093) 190-53-79, e-mail: chigozieikwuegbu@yahoo.com;

The goal of the paper is to analyze the concept of cloud and how to benefit from this technology in an academic environment. In order to develop an e-learning platform academic purposes, new methodologies should be considered for the research. An academic cloud framework is proposed in order to provide a new era in e-learning. This framework addresses the services and deployment of cloud in a new dimension and each layer specifies the benefits and significance and essential components needed to construct an academic cloud.

The cloud is an Information Technology (IT) practice of using a network of remote servers hosted on the Internet to store, manage and process data rather than a local server or personal computer. Nowadays there are many users, companies, business which use different cloud platforms for achievement of their goals. The most used cloud platform is Software as a Service (SaaS) [1].

For development and implementation of SaaS platform, a web application is needed to be developed because hosting a web application is a business that provides the technologies and services needed for the web application to be viewed on the Internet. Web applications are hosted on special computers called serves and when we input the domain into our browsers, we are connected to the server. The following are a few things to consider when building a web application and hosting it [2].

1. Designing a Software System describes vendor neutral best practices for hosting web applications in the cloud. The main idea of this step is to choose types of hosting environments of cloud: private, public or hybrid.
2. System Architecture describes the components required by the application to be hosted. These elements support the different types of cloud systems and they include:
   - Load Balancing. This allows to spread load across multiple resources such as computers processors and storage or network link.
   - Firewalls with Security Groups. This brings about security, providing a host-level firewall both on the web servers and the application servers.
   - Content Delivery Network. These are geographically distributed systems of servers deployed to minimize the response time for serving resources to geographically distributed users ensuring that content is highly available with minimum latency.

- Managed Databases. These are a structured set of data. Typically, there are kept storage devices connected to computers and/ or networks.
- DNS Services: Domain Name System server resolves the text URL for a particular web resource to the TCP/IP address of the system or service which can deliver the resource to the client.
- DDoS Protection. This is a means to safeguard infrastructure against multiple compromised systems which is the most common network and transport layer distributed denial of service attack.

3. Hosting a web application. When considering hosting a web application, one needs to consider a number of things which range from cost, scalability. Many web applications contain some form of persistence, usually in the form of a relational or NoSql database. Selecting a solution that offers both is essential.
4. To effectively develop a software, it is required to gather the requirements of the application from the user. The user does this by using mind mapping applications to put down all the specifications of the software to be developed. This includes number of users able to access the application, level of security, authentication, colors present in the application [3].

Conclusion

So, cloud computing is becoming a regular concept nowadays. Many companies accelerate their pace of development in the cloud computer systems and improving their services to meet a wide range of users. Deploying web applications such as lecture schedule, conferences, and lecture material would be beneficial for students such that they would be able to access what they need easily. It would give them the opportunity to do more learning outside the classroom.

List of references

[1] J. Surbiryala, C. Li and C. Rong, "A framework for improving security in cloud computing," *2017 IEEE 2nd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA)*, Chengdu, 2017, pp. 260-264.
[2] B. Russo, L. Valle, G. Bonzagni, D. Locatello, M. Pancaldi and D. Tosi, "Cloud Computing and the New EU General Data Protection Regulation," in *IEEE Cloud Computing*, vol. 5, no. 6, pp. 58-68, Nov./Dec. 2018.
[3] G. Kulkarni, J. Gambhir, T. Patil and A. Dongare, "A security aspects in cloud computing," *2012 IEEE International Conference on Computer Science and Automation Engineering*, Beijing, 2012, pp. 547-550.

МЕХАНІЗМ РЕАЛІЗАЦІЇ АТАКИ ТИПУ MAN-IN-THE-MIDDLE НА ПРОЦЕС SLAAC IPv6

Калінєнкова А.Л.
Науковий керівник – к.т.н., доцент Снігуров А. В.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки,14, каф. Інфокомунікаційної інженерії,
тел. (057) 702-13-20), E-mail: anastasiia.kalinienkova@nure.ua

Internet network is a giant network of computers around the world. The billions of devices are constantly connected to each other for the information transmission and reception. The IP address is used for identifying the device on the Internet and route traffic to specific devices. IPv6 network protocol is an improved IPv4 replacement, which will soon end the address space. Now the world is in the conditions where IPv6 becomes an integral part of the network environment, which means attacks will be more frequent.

Актуальність теми дослідження. в кінці лютого 2018 року була зафіксована перша масштабна DDoS-атака по протоколу IPv6. Постраждала UltraDNS - DNS-мережа компанії Neustar, яка обробляє 10% всього інтернет-трафіку. Перехід на протокол IPv6 підтримують світові провайдери та інтернет-компанії, відповідно до цього можна прогнозувати зростання кількості кібератак по даному протоколу.

Мета дослідження. Аналіз існуючої вразливості у протоколі IPv6 – SLAAC, яка дає можливість провести атаки типу MitM на ураження функціональності та розкриття конфіденційної інформації, яка передається.

Для проведення однієї з найефективніших атак зловмиснику потрібно розмістити та приєднати свій IPv6-маршрутизатор до спеціальної мультикаст-групи FF02::2, запустити DHCPv6-сервер (для конфігурації вузлів версії 6 з IP-адресами, префіксами IP), DNSv6 (мережевий протокол для налаштування хостів Інтернет-протоколу версії 6 з IP-адресами, префіксами IP) і NAT64-транслятор.

Як тільки будь-який маршрутизатор приєднається до спеціальної мультикаст-групи FF02::2, він відразу ж починає розсилати RA повідомлення про об'яву маршрутизатора (далі - RA) (рисунок 1). Cisco-маршрутизатори розсилають їх кожні 200 с. за замовчуванням. Нюанс полягає в тому, що клієнтам не потрібно чекати 200 с., вони відправляють RS повідомлення запиту маршрутизатора (далі - RS) на ці мультикаст-адреса і таким чином негайно вимагають всю інформацію.

Якщо маршрутизатору зловмисника вдасться вставити себе в RA повідомлення, він зможе підробити оголошення маршрутизатора ICMPv6 від маршрутизатора клієнта, яке встановлює час життя повідомлення 2 години. Згідно RFC 4862, «якщо час RemainingLifetime менше або дорівнює 2-м годинам, ігноруйте параметр «Інформація про префікс» щодо

дійсного часу роботи, якщо тільки оголошення маршрутизатора, з якого отримано цей параметр, не було аутентифіковано». Це може привести до припинення роботи адреси маршрутизатора клієнта через 2 години, і маршрутизатор зловмисника зможе потім відправити оголошення нового маршрутизатора з новим префіксом (відображається як 2001:DB8:BAD::/64). Побачивши новий префікс, маршрутизатор клієнта вибере нову адресу (показану як 2001: DB8:BAD::A).

Рисунок 1 – Етапи атаки SLAAC IPv6

Перехопивши RS запит маршрутизатора клієнта, зловмисник може підмінити RA відповідь маршрутизатора і вказати у відповіді підроблені налаштування. В якості шлюзу за замовчуванням зловмисник вказує свій пристрій, і весь трафік клієнта, який передається в зовнішні мережі, буде проходити через атакуючого. Згодом, завдяки механізму Stateless Address Autoconfiguration (далі - SLAAC) пристрої отримують свій префікс, довжину префікса і адресу шлюзу від IPv6 маршрутизатора зловмисника.

Пристрій зловмисника виступить в якості проксі сервера між клієнтом і зовнішніми мережами. При цьому весь трафік, який проходитиме через маршрутизатор зловмисника, схильний до атаки MITM, також тому, що зловмисник може призначити помилковий DNS сервер внутрішнім хостам. Невірний DNS-сервер дозволить зловмиснику перенаправити весь внутрішній трафік на будь-яку кількість фішингових сайтів.

Висновки. Результати роботи пропонується використовувати для створення математичної моделі даної атаки, а також розробки механізмів захисту системи маршрутизації від кібератак.

Література:

1. IPv6 First-Hop Security Concerns – [Електронний ресурс]. – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/about/security-center/ipv6-first-hop.html?fbclid=IwAR0yGa_0cSR4HJjhWh2cdZI4kWf8997rtkHOu6HawsBppPVvT7lXomD3JQ#5a.
2. IPv6 — это весело, часть 2 – [Електронний ресурс]. – Режим доступу до ресурсу: https://habr.com/ru/post/254293/.

НОВИЙ ПІДХІД ДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ВЕБ-РОЗРОБЦІ ВІД SQL ІН'ЄКЦІЙ

Кацан М.Р.
Науковий керівник – к.т.н., доцентФурса С.Є.
Донецький Національний університет імені Василя Стуса
(21021, Вінниця,вул. 600-річчя, 21, каф. Радіофізики та кібербезпеки, тел. 0938920942)
katsan.misha.r@gmail.com

The article discusses the information security issues and their protection in cases of SQL injections. A number of recommendations how to reduce applications vulnerability is suggested in the theses. Also the article outlines a few ways how to prevent SQL injections using new web application development standards.

Сьогоднішній день характеризується активним застосуванням інтернету у всіх без виключень сферах людського життя. Тому всі розробники намагаються максимально доступно робити веб-додатки. При цьому також необхідно подбати про безпеку сайту, цілісність та доступність інформації користувачів та самого контенту сайту. Зокрема, питання безпеки баз даних досі є актуальним. Так, згідно статистичних даних міжнародної компанії «Positive Technologies», що спеціалізується на розробці програмного забезпечення в галузі інформаційної безпеки,SQLін'єкції залишаються на вершині рейтингу.

В більшості випадків, зловмисники намагаються отримати доступ до якоїсь певної бази даних веб-додатку. Але не завжди вона там може бути єдиною. В такому випадку за допомогою SQLін'єкцій можна отримати доступ до всіх баз, що зберігаються на сервері[1]. Адже розміщення веб-додатку на сервері не означає, що база даних буде знаходитися там же.

На практиці використовують нові технології для розробки на стороні клієнта окремо від серверної обробки програм. Інакше кажучи, це Front-end – сторона клієнта та Back-end–сторона сервера. Зазвичай Front-endвідправляє запити на Back-end, сторона сервера, після того як обробляє ці запити, виконує відповідні дії. Даний зв'язок відбувається за допомогою ApplicationProgrammingInterface (API) – прикладного програмного інтерфейсу. І в таких випадках на сервері зберігається декілька баз. Відповідно, даний спосіб атаки дасть доступ до всіхких баз.

Існує три основні категорії атак– вбудовані(In-bandSQLi), виведені(InferentialSQLi) тапозаканальні(Out-of-bandSQLi)[2], які були розглянуті суто практично. Для цього було реалізовано прототип сайту книжкової крамниці,в якому є форма авторизації, де користувач вводить свій логін та пароль, після чого потрапляєусвій особистий кабінет, девідображаються куплені та доступні йому книги.В подальшому на базі розробленого додатку потрібно досліджувати відправлення не лише з

форми авторизації, а також при сортуванні, виборі статті при реєстрації, адже всі ці дані будуть оброблятися веб-додатком і навіть найпростіші з них можуть зробити додаток вразливим. Враховуючи вищевикладене, запропоновано такі рекомендації для запобігання виникненнюSQLін'єкцій:

- Не використовувати динамічний SQL (Уникати розміщення даних з полів вводу безпосередньо в операторах SQL).
- Надавати перевагу підготовленим твердженням та параметризованим запитам, які набагато безпечніші.
- Фільтрувати введені дані.
- Уникати не бажаних символів.
- Перевіряти типи очікуваних даних.
- Конфіденційні дані мають бути представлені в зашифрованому вигляді.
- Створити права доступу до бази даних.
- Встановити мінімальні можливості для користувачів, які взаємодіють з базою даних.
- Відключити відображення помилок бази даних безпосередньо для користувачів (зловмисники можуть використовувати ці повідомлення про помилки, щоб отримати інформацію про базу даних).
- Оновлювати бази даних до останніх доступних версій (це запобігає використанню зловмисників відомих недоліків або помилок у старих версіях).

Показано, що наслідки нереалізованого розробником фільтрування введених даних від користувачів можуть призвести до втрати даних з усіх баз, які є на даному сервері, навіть, якщо вони не відносяться до даного додатку, що на практиці трапляється досить часто.

Використана література:

1) SQL Injection. URL: https://www.owasp.org/index.php/SQL_Injection (last accessed: 24.02.2019)
2) Understanding SQL Injection. URL: https://www.cisco.com/c/en/us/about/security-center/sql-injection.html (last accessed: 24.02.2019).

REMOTELY CONTROLLED MINDSTORM NXT VEHICLE USING BLUETOOTH COMMUNICATION

Obot E.I.
Scientific supervisor – Ass. Prof. Yevdokymenko M.O.
Kharkov National University of Radio Electronics
(Infocommunication engineering Department, 14, Nauky Ave., Kharkov,
Tel. (063)327-60-70), e-mail: obot.edidiong.ime@nure.ua

This paper presents the remote control of the Lego car using a personal computer (PC) via Bluetooth communication. The system presented here consists of a PC, a Lego MINDSTORMS car, and a program to be run on the PC to connect to the Lego MINDSTORMS car and to send commands to the Lego car. This program is written in Java on leJOS NXJ. An Android smartphone is used to capture the view in front of the robot. It mounted in the holder streams video through the Internet, so it can be viewed in real-time on the PC. The purpose of this paper is the development a small scale remote controlled vehicle using a Bluetooth communication and vision system from the idea to the final testing.

A remote control vehicle is defined as any vehicle that is Teleported by a means that does not restrict its motion with an origin external to the device. This is often a radio control device, cable between control and vehicle, or an infrared controller. A remote control vehicle (RCV) differs from a robot in that it is always controlled by a human and takes no positive action autonomously [1].

One of the key technologies which underpin this field is that of remote vehicle control. It is vital that a vehicle should be capable of proceeding accurately to a target area manoeuvring within that area to fulfil its mission and returning equally accurately and safely to base.

A relatively new research area in remote control concerns the communication technology for the control of the vehicle in conjunction with other devices or between a team of vehicles. A good communication system between the user and the RCV will expand the capability and versatility of vehicles. In this project, wireless communication allows a RCV to be used as a part of more complex systems or to interact with the user using common equipment (e.g. remote controller).

One way for design of remotely controlled vehicle using Bluetooth communication for the robot is using LEGO MINDSTORMS NXT. This little turbo charged radio controlled car uses analogue steering. Using the term turbo because the gears speed up motor rotation 1.67 times. The navigation problem can be solved by using a camera of Android smartphone.

To achieve this goal, the following tasks need to be addressed:

1. To choose a platform for realization of the remote controlled vehicle;
2. To choose a CAD tools for design of the remote controlled vehicle;
3. To propose system architecture;

4. To design chassis of the remote controlled vehicle;
5. To design embedded system of the remote controlled vehicle;
6. To design communication programs of the remote controlled vehicle with vision system;
7. To evaluate the performance of the developed remote controlled vehicle.

Problems encountered whilst testing and building the robot are the robot travels the slower and weaker the connection due to the limited distance of a Bluetooth connection which is (10 metres); the weight of the smartphone didn't really suit the robot it kept weighing the robot down and it probably won't move properly because of this; the platform where the robot was tested it wasn't smooth and plain enough so there was a bit of discomfort operating the robot in that condition. Experimental results of the paper is shown on figure 1.

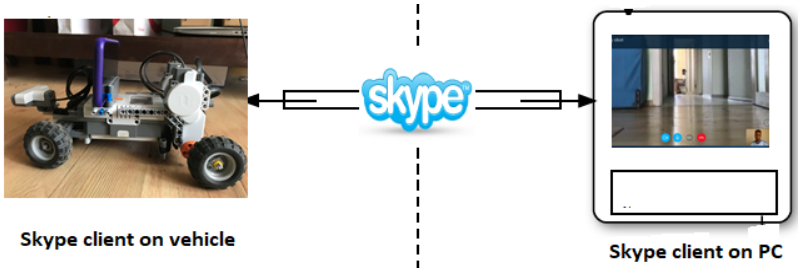


Fig.1 – Architecture monitoring subsystem as experimental result

Conclusion

1. Developing efficient software using the NXT-G software based on visual programming.
2. Valuable experience of both learning robotics and embedded systems design using Lego Mindstorm platform.
3. Learnt a tremendous amount about motor control systems.
4. Building robots with different design that can execute different tasks.

List of references

1. S. Kahar, R. Sulaiman, A. S. Prabuwono, M. F. M. Amran and S. Marjudi, "Data transferring technique for mobile robot controller via mobile technology," *2011 International Conference on Pattern Analysis and Intelligence Robotics*, Putrajaya, 2011, pp. 103-108.
2. B. Jincun, L. Qi and L. Yanfei, "The Design of the Rescue Robot Long-Distance Control Based on 3G and GPS," *2009 International Conference on Intelligent Human-Machine Systems and Cybernetics*, Hangzhou, Zhejiang, 2009, pp. 170-172.
3. M. B. Perotoni, B. E. Garibello and S. E. Barbin, "An IEEE802.11 low cost planar antenna for a mobile robot," *2006 IEEE Antennas and Propagation Society International Symposium*, Albuquerque, NM, 2006, pp. 969-972.
4. F.Cleveland, "Use of wireless data communications in power system operations," in Proc. 2006 IEEE Power System Conf. and Expo., pp. 631-640.

SECURITY SOFTWARE DEVELOPMENT FOR ARDUINO-ROBOT MOTION CONTROL

Olaide Jamiu Olalekan
Scientific supervisor – Ass. Prof Yevdokymenko M.
Kharkov National University of Radio Electronics,
Infocommunication engineering Department, 14, Nauka Ave., Kharkov,
Tel. (063) 063-07-82, e-mail olaide.jamiu@nure.ua

The given work is devoted to the software development for Arduino-Robot motion control. There is considered the mobile robotics application, the general approach to a mechanical design, security software mechanisms for developing, the description of Arduino-Robot platform and the methods of motion control is explained. The main steps for development Arduino-Robot is described in this paper. During execution, these steps it is developed the software for Arduino-Robot control with application of different motion algorithms and programming procedures.

Mobile Robotics is an active long research, where people find new technologies to improve mobile robots intelligence and application. Robots now move in a dynamic way where they are autonomous.

Locomotion is a method that robots use to transport themselves from place to place, a major goal in this field is in developing capabilities for robots to autonomously decide how, when, and where to move. Autonomous robot locomotion is a major technological obstacle for many areas of robotics, such as humanoid. Types of locomotion include walking, running, hopping, swimming, sailing, flying, skating etc. Moreover, one of the popular approach for the development of mobile robotics is used based on Arduino platform. Because Arduino is an open source computer hardware and software community that manufacture and design microcontroller kits for building digital devices and objects that can sense and control object in physical world.

For achievement of aim of this paper was done such steps, as: considering the mobile robotics application; considering description of Arduino Robot platform, different types of Arduino hardware and the IDE, advantages and problems; development the Software for Arduino Robot control with application of different motion algorithms and programming procedures [1-2].

According to this aim of the paper, the following steps are assigned:

- Mobile robot and Arduino.
- Installation.
- Development of coordinates and line following.
- Range finder.

The aims and assignment were all appropriately done and made visible and possible because of the availability of the robot language allowing us to

program the microcontroller enhancing the use of an open source Arduino application which has the libraries needed to achieve the listed goals.

The program were written and implemented with the aid of integrated development environment enabling connection between the application and the microcontroller with the use of a USB cord which is a direct link to program the microcontroller. Thus this allows the full implementation of the aim listed above and the Arduino robot fully understand the programming language and perform the function needed [3-4].

Conclusion

The main aim of the project was to realize the use of Arduino platform to make an approach on mobile robot. This is a huge impact in the world as a whole where robot literally does all the dangerous work a man is meant to do be in industrial purpose, medical purpose and a lot more. Here in the project we are fortunate to use Arduino as a whole concept of the project and see how it helps in robotics.

The issue of security is needed to secure our code from being corrupted or turn invalid, the security mechanism is added to the on-board microcontroller, to signal overloading of data to the chip.

List of Reference

[1] R. Connaughton and M. Modlin, “A modular and extendable robotics platform for education,” in Frontiers in Education Conference, 2009. FIE’09. 39th IEEE, 2009, pp. 1–4.

[2] M. Rubenstein, C. Ahler, and R. Nagpal, “Kilobot: A low cost scalable robot system for collective behaviors,” in Robotics and Automation (ICRA), 2012 IEEE International Conference on, 2012, pp. 3293–3298.

[3] F. Mondada, M. Bonani, X. Raemy, J. Pugh, C. Cianci, A. Klaptocz, S. Magnenat, J. christophe Zufferey, D. Floreano, and A. Martinoli, “The e-puck, a robot designed for education in engineering,” in In Proceedings of the 9th Conference on Autonomous Robot Systems and Competitions, 2009, pp. 59–65.

[4] J. McLurkin, J. Rykowski, M. John, Q. Kaseman, and A. J. Lynch, “Using multi-robot systems for engineering education: Teaching and outreach with large numbers of an advanced, low-cost robot.” IEEE Trans. Education, vol. 56, no. 1, pp. 24–33, 2013.

МЕТОДИ БЛОКУВАННЯ САЙТІВ

Семенченко О. А.
Науковий керівник – д.т.н. доцент Золотарьов В. А.
Харківський національний університет
Радіоелектроніки
(61166, Харків, пр. Науки,14, каф. Інформаційно-мережна інженерія,
тел. (057) 702-13-06)
e-mail: oleksandr.semenchenko@nure.ua, +380507683086

In today's world, billions of people are facing a form of blocking when surfing the internet. Access to Internet content in countries is blocked using Internet service providers. Individual countries resort to technical restriction of access, usually for reasons of national security and to implement specific laws.

Many users are also blocking access to resources that have been blocked for various reasons.

By comparing all kinds of blocking and bypassing the blocking of sites, I brought them a classification. Also, for each criterion I have assigned my coefficient.

У сучасному світі мільярди людей стикаються з тією чи іншою формою блокувань при серфінгу в інтернеті. Доступ до інтернет-контенту в країнах блокується за допомогою обладнання інтернет-провайдерів. До технічного обмеження доступу окремі країни вдаються, як правило, з міркувань національної безпеки і з метою виконання конкретних законів.

Громадська організація Internet Society виділяє кілька способів блокування доступу до інтернету, серед яких: блокування по IP, блокування сайту по URL, блокування із застосуванням системи DPI, блокування в рамках конкретних платформ (особливо пошукових систем) і блокування по DNS.[1]

Також багато користувачів обходять блокування для отримання доступу до ресурсів які були заблоковані за різними причинами. Найвідоміші методами являються:використанняCGI-proxy,DNS, перекладача, VPN, кеш Google, зміни IP-адреси або використання браузеру TOR

Порівнюючи усі види блокування та обходу блокування сайтів я привів їх класифікацію. Також кожному критерію я присвоїв свій коефіцієнт. Найменше значення яке ми отримаємо в сумі усіх коефіцієнтів тим краще.

Коефіцієнтами являлись:

- Кваліфікація, які необхідні навики для блокування чи розблокування ресурсу;

- програми, які необхідні для блокування чи розблокування ресурсу;
- апаратура, яка необхідна для блокування чи розблокування ресурсу;
- умови можливості блокування та розблокування мається на увазі можливості блокування, а саме на який період ми заблокуємо даний ресурс, чи розблокування.

В кінці можна зазначити, що усі способи блокування мають два загальні недоліки:

1. Вони не вирішують проблему Блокування не видаляє контент з Інтернету, не перешкоджає незаконній діяльності і не допомагає переслідувати злочинців; вона усього лише приховує контент від очей широкої публіки. Сам по собі контент нікуди не зникає.

2. Вони заподіюють непрямий збиток Кожен спосіб блокування і надмірний, і недостатній одночасно - неминуче блокується дозволений контент і пропускається заборонений. Проте збиток Інтернету цим не обмежується - блокування збільшує риски кінцевих користувачів, пов'язані із спробами обійти блокування, знижує прозорість Інтернету, руйнує атмосферу довіри, заганяє інтернет-служби в підпіллі і вторгається в приватне життя користувачів. Крім того, необхідно враховувати усі витрати, пов'язані з блокуванням.

Література:

1. Закон України «Про основні засади забезпечення кібербезпеки України» // (Відомості Верховної Ради (ВВР), 2017, № 45, ст.403
2. Конвенція Ради Європи «Конвенція про кіберзлочинність» // http://zakon.rada.gov.ua/laws/show/994_575
3. Стратегія кібербезпеки України», затверджена Указом Президента України від 15 березня 2016 року № 96/2016. // http://zakon.rada.gov.ua/laws/show/96/2016#n11
4. Internet Society «Internet Society — обзор перспектив блокировкиинтернет-контента» 2017р.

ОПЕРАЦІЙНІ РИЗИКИ ІНФОКОМУНІКАЦІЙНОЇ БАНКІВСЬКОЇ СИСТЕМИ

Стрекозова Ю. І.
Науковий керівник – к.т.н, доц. Золотарьов В. А.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Леніна, 14, каф. Інформаційно-мережної інженерії,
тел. (057) 702-14-29)
e-mail: yuliia.strekozova@nure.ua

The main purpose of managing operational risks of the infocommunication banking system is to ensure their reliability and security. This is due to the desire of banking organizations to meet the needs of customers that arise with the development of their business, in particular, rolling national borders and which require a wide range of banking operations using information systems. The relevance of the research topic is that the regulation of the risk of using information and telecommunication systems is now becoming one of the most important factors ensuring the stability of the banking system.

Основою успішної банківської діяльності є оптимізація параметрів інформаційних ризиків, що викликає потребу у комплексному підході до системи управління ними [1]. Сьогодні банки направляють значні зусилля на розширення структури управління операційним ризиком в компанії і намагаються співвіднести операційний ризик безпосередньо з ризиковим капіталом, який вони підтримують для покриття непередбачених втрат. **Операційний ризик** - це ймовірність виникнення збитків або додаткових втрат або недотримання запланованих доходів внаслідок недоліків або помилок в організації внутрішніх процесів, навмисних або ненавмисних дій користувачів, збоїв у роботі інфокомунікаційних систем банку або внаслідок впливу зовнішніх факторів.

Для управління операційними ризиками в інфокомунікаційних банківських системах застосовують наступні методи:

самооцінка операційних ризиків — періодична оцінка ризиків, що супроводжують діяльність бізнес-напрямів, персоналом цього напряму, це, крім оцінки загроз, сприяє розвитку культури розуміння небезпек серед персоналу;

оцінка електронного бізнесу з урахуванням ризиків — оцінка бізнес-напрямів з урахуванням супутніх ризиків, внаслідок чого визначається реальна «рентабельність» бізнес-напрямів, критичні процеси, пріоритети для використання ресурсів і додаткових заходів контролю;

розвиток інфокомунікацій з урахуванням ризиків — всі істотні зміни бізнес-процесів, зокрема впровадження нових продуктів і послуг, мають супроводжуватися оцінкою наявних і потенційних ризиків для визначення чутливості процесу до ризику;

ведення бази даних операційних інцидентів і збитків — усі операційні інциденти, пов'язані з операційним ризиком, а також операційні збитки внаслідок таких інцидентів, повинні бути зафіксовані в базі даних для оцінки і розробки заходів щодо запобігання таких інцидентів і збитків у майбутньому;

звітність за ризиками — усі відомості про операційні ризики, зокрема щодо оцінки ризиків та їх покриття капіталом, а також операційних інцидентів і збитків, мають бути відображені у звітності банку з урахуванням суттєвості ризику/інциденту/збитку для банку [2].

Мета управління операційними ризиками - побудова культури управління операційним ризиком та внутрішнього контролю, мінімізація збитків банку від реалізації операційного ризику, оптимізація та удосконалення процесів та продуктів банку, підвищення репутації банку та забезпечення найвищого рівня захисту коштів клієнтів та акціонерів банку, отримання високих національних та міжнародних рейтингів стабільності та надійності банку, підтримки міжнародних організацій, вигідних умов для залучення ресурсів [2].

Система управління операційним ризиком - сукупність належним чином задокументованих і затверджених політик, методик, порядків і процедур управління операційним ризиком, які визначають порядок дій, спрямованих на здійснення систематичного процесу виявлення, вимірювання, моніторингу, контролю, звітування та пом’якшення операційного ризику на всіх організаційних рівнях банку [3].

Перелік джерел:

1. Сайт Національного центру підготовки банківських працівників [Електронний ресурс] Режим доступу: www/ URL: http://www.nctbpu.org.ua/main/index/ua/activities/retraining/risks - 19.02.2019 р. – Загол. з екрану

2. Сайт Путівник [Електронний ресурс] Режим доступу: www/ URL: https://my.privatbank.ua/other_instructions/232/5 - 19.02.2019 р. – Загол. з екрану

3. Сайт Bankchart.ua [Електронний ресурс] Режим доступу: www/ URL: http://www.bankchart.com.ua/mizhbankivskiy_biznes/statti/bankivski_operatsiyni_riziki_yak_dobre_vmiti_rahuvati 19.02.2019 р. – Загол. з екрану

ІНФОКОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ

АНАЛІЗ СПЕКТРАЛЬНОЇ ЭФФЕКТИВНОСТИ СОЛИТОННЫХ ЕФЕКТИВНОСТІ СОЛІТОНИХ ВОЛЗ НА ОСНОВІ ФОТОННО-КРИСТАЛІЧНИХ ВОЛОКОН

Абіх І.В.
Науковий керівник – к. т. н., доц. Колтун Ю.М.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. «Інформаційно-мережна інженерія»,
тел. (057) 702-14-29; e-mail: iryna.abikh@nure.ua)

The most important factors that affect throughput and communication range in modern fiber optic lines are the presence of nonlinear effects the fibers. One method of reducing the effects of nonlinear effects, and namely: increasing the ratio of the data transfer rate to the width spectral channel with an increase in signal power or spectral efficiency, is the use of solitons as pulses, carrying information. This report is devoted to the analysis of spectral the efficiency of soliton fiber based on photonic crystal fibers, what is the actual task.

Сьогодні основною тенденцією розвитку телекомунікацій є постійне збільшення обсягів інформації, що передається. Це викликане постійно зростаючою кількістю додатків і послуг, які задовольняють концепції «Triple-Play Services». Ця концепція відображає обмін інформацією, що подається в трьох видах: мова, дані і відео, а надання такого роду послуг вимагає високої якості, великої пропускної здатності і дальності зв'язку. Виконання цих вимог можуть забезпечити волоконно-оптичні лінії зв'язку (ВОЛЗ).

У цьому аспекті важливо розуміти фізичні процеси і закономірності, що виникають у процесі поширення сигналів в оптичному волокні (ОВ). Зокрема факторами, що впливають на пропускну здатність і дальність зв'язку в сучасних ВОЛЗ є наявність лінійних і нелінійних ефектів у ОВ. Якщо для зменшення лінійних спотворень в ОВ, що викликані оптичними втратами і дисперсійними впливами, вже існують практичні методи на основі ербійових підсилювачів і компенсаторів дисперсії, то для зменшення нелінійних ефектів таких методів немає, а їх створення і дослідження є актуальною задачею [1].

Одним з методів зменшення впливу нелінійних ефектів, а саме: підвищення параметра відношення швидкості передачі даних до ширини спектрального каналу у разі зростання потужності сигналу або спектральної ефективності є використання солітонів, в якості імпульсів, що переносять інформацію [2]. Такий імпульс утворюється за рахунок взаємної компенсації дисперсії і нелінійності, що робить його більш стійким для передачі інформації у нелінійному середовищі ОВ.

У доповіді аналізується спектральна ефективність солітонних ВОЛЗ на основі фотонно-кристалічних волокон (ФКВ). Такі ОВ являють собою мікроструктурні або дірчасті волокна, в яких головною складовою є

фотонні кристали (ФК) – неоднорідні діелектрики з періодичної варіацією коефіцієнта рефракції. Особливістю ФК є наявність фотонної забороненої зони, тобто діапазону частот, в межах якого світло не може проникати крізь його структуру [3].

Для опису поширення електромагнітної хвилі по ФКВ було використане узагальнене нелінійне рівняння Шредінгера [1, 2]:

$$\frac{\partial A}{\partial z} = -\frac{\beta_2}{2}\frac{\partial^2 A}{\partial t^2} + i\gamma|A|^2 A + iN(z,t),$$

де A (z, t) – комплексна обвідна амплітуди поля; t – час; z – відстань уздовж ОВ; β_2 - параметр хроматичної дисперсії, γ – параметр нелінійності. Член рівняння N (z, t) описує генерацію шуму, що виникає внаслідок оптично підсиленої спонтанної емісії [2].

Проведений аналіз показав, що в області високих значень відношення сигнал/шум (SNR) солітонні ВОЛЗ, що використовують ФКВ, мають велике значення спектральної ефективності. Зазначено, що при одному і тому ж значенні спектральної ефективності можлива передача сигналу на великі відстані в порівнянні з передачею по ВОЛЗ, які організовані на стандартному ОВ.

Також були проаналізовані основні ефекти, які обмежують зростання спектральної ефективності солітонних ВОЛЗ, такі як ефекти Гордона-Хауса і Гордона-Молленауера, що проявляються у випадковому відхиленні положення центру імпульсу і його фази відповідно від початкового значення.

Таким чином, в доповіді наведені принципові можливості солітонних ВОЛЗ, проведене їх порівняння з традиційними оптичними лініями, проаналізовані причини зменшення спектральної ефективності у разі зростання відношення сигнал/шум.

Список джерел

1. Юшко О.В. Солитонные линии связи на основе спектрально-эффективных форматов модуляции / О.В. Юшко, А.А. Редюк // «Квантовая электроника». – 2014. – №6. – С. 606 – 611.

2. Юшко О.В. Математическое моделирование солитонных волоконно-оптических линий связи / О.В. Юшко, А.А. Редюк, М.П. Федорук, С.К. Турицын // Материалы Российского семинара по волоконным лазерам. – 2014. – С. 107 - 108

3. Абдурахман А. Использование фотонно-кристаллического волокна в телекоммуникационных системах / А. Абдурахман // Технологический аудит и резервы производства. – 2016. – № 3/2 (29). – С. 62 – 67.

СУЧАСНІ НАПРЯМКИ РОЗВИТКУ ХМАРНИХ ОБЧИСЛЕНЬ

Галушка А.В.
Науковий керівник – к.т.н., доц. Костромицький А.І.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки,14, каф. Інформаційно-мережної інженерії,
тел. (057) 702-14-29)
e-mail: andreygshadow@gmail.com, тел (057) 702-11-13

The characteristics of the current state of the cloud services market, the main models of service provision and infrastructure deployment models are given. The analysis of the main directions of scientific researches of cloud computing has been carried out. On the basis of the analysis of open sources, some features of the current stage of development of scientific research in this field are determined, in particular, a significant proportion of these studies are conducted using experimental methods and approaches.

Останні приблизно півтора десятиріччя відбувається надзвичайно бурхливий розвиток хмарних сервісів. Вони пройшли шлях розвитку від початкової концепції IaaS (Infrastructure as a service, інфраструктура як сервіс), далі до PaaS (platform as a service, платформа як сервіс) та SaaS (software as a service, програмне забезпечення як сервіс). На цих класичних концепціях розвиток не зупинився і зараз можна сказати, що набула популярності концепція XaaS (усе в хмарі). Оскільки не всі пропоновані хмарні сервіси можна однозначно віднести до вказаних вище, виникли такі концепції як BaaS (бекенд як послуга), FaaS (функція як послуга) та багато інших.

Розвиваються не тільки моделі обслуговування, але й моделі розгортання інфраструктури – є моделі приватної, публічної, громадської, гібридної, персональної хмари, суперхмари тощо.

Аналіз відкритих маркетингових даних свідчить про те, що ринок хмарних сервісів в Україні зростає вже не менше шести років поспіль, що в цілому відповідає загальносвітовим тенденціям. Так, у 2018 році обсяг глобального хмарного ринку перевалив за $ 250 млрд, збільшившись на 32% щодо 2017-го. Відповідно відбувається постійне зростання як кількості центрів обробки даних (ЦОД), так і обчислювальної потужності та пропускної здатності вже існуючих центрів.

В цих умовах постійно зростаючої конкуренції, фактично на глобальному ринку, ефективність роботи інфраструктури, платформи, сервісів зокрема та хмари в цілому стає дуже важливим та актуальним питанням для власників цього бізнесу. Хоча в багатьох рекламних матеріалах та в результатах досліджень вказується, що використання хмарної інфраструктури дозволяє знизити витрати підприємства на підтримку інфраструктури в порівнянні з використанням власної інфраструктури, ще значна частка підприємств продовжує надавати

перевагу варіанту використання власної інфраструктури. Подальше підвищення ефективності хмарних обчислень безумовно сприятиме частковому або навіть повному переходу таких підприємств до моделі використання хмарних сервісів.

Зазначимо, що ефективність роботи хмари слід розуміти в широкому сенсі. Тематика наукових досліджень в цій галузі охоплює достатньо широке коло питань, які безпосередньо чи опосередковано впливають на ефективність.

Можна виділити такі сучасні напрямки розвитку хмарних обчислень, як:

- вдосконалення енергоефективності інфраструктури;
- забезпечення різних аспектів хмарної безпеки;
- вдосконалення архітектури хмарних обчислень;
- пошук нових та вдосконалення існуючих сервісів;
- підвищення конкурентоспроможності хмарних послуг;
- вдосконалення моделей обслуговування користувачів хмарних сервісів тощо.

Дуже перспективними є дослідження алгоритмів обробки великих даних, дослідження в галузі Інтернету речей та штучного інтелекту, машинного навчання.

В цілому актуальність наукових досліджень в галузі хмарних обчислень має зростаючий тренд. Проте, значна частка наукових публікацій по хмарним обчисленням переважно зосереджена на технологічних підходах та інструментах. А таким важливим аспектам як бізнес, концептуальна і прикладна область приділяється значно менша увага.

Ще однією з особливостей наукових досліджень в галузі хмарних обчислень є те, що значна їх кількість не підкріплена теоретичними положеннями і концептуальними моделями. Крім того, більшість досліджень хмарних обчислень використовували експеримент і моделювання в якості методів дослідження, а менша частина - якісні, кількісні і змішані методології.

В доповіді автор даних тез дає характеристику сучасному стану ринку хмарних сервісів, основних моделей надання послуг та розгортання інфраструктури, основним напрямкам наукових досліджень хмарних обчислень та особливостям сучасного етапу розвитку наукових досліджень в цій галузі.

В якості висновку можна відзначити, що центри обробки даних є основою хмарних обчислень, отже аналіз сучасних теоретико-методологічних та практичних підходів до організації роботи ЦОД є основою для знаходження шляхів підвищення ефективності хмарних обчислень.

ВИКОРИСТАННЯ БЛОКЧЕЙНУ ТА СМАРТ-КОНТРАКТА ЯК БЕЗПЕЧНЕ КЕРУВАННЯ РОБОЧИМ ЧАСОМ

Йолкін Г. І.
Науковий керівник – д.т.н., проф. Олійников Роман Васильович
Харківський національний університет імені В. Н. Каразіна
(61022, Харків, майдан Свободи 4, каф БІСТ тел: +38 (057) 707-55-00)
E-mail: info@karazin.ua , botgen@gmail.com , Факс: +38 (057) 705-02-41,
моб +380932950493

The given work is devoted to the modern developments and using blockchain with smart-contracts as management system (based SCRAM) and new vision by using Cryptocurrency.

- payment only for the task;
- guarantee of receiving wages;
- stabilization of assets;
- cumulative program;
- trust between two or more parties that do not trust each other;
- protection against inflation;
- flexible tax control;
- open, transparent, understandable, accessible assessment system.

Моделирование управления проектами в глобальной компании методом управления подобным SCRAM, где ответственность за выполнение берёт механизм на основе умных контрактов (smart contract).

Создание корпоративных токенов так называемой криптовалюты на основе блокчейна со смарт-контрактами для управлением рабочим временем либо инвестиций, которые не смогут потерять в цене из-за того что эта самая единица, токен (taskcoin) будет приравнена к денежному эквиваленту минимальной оплаты труда.

Как тестовая система реализуется созданием собственной, корпоративной, криптовалюты на основе платформы Ethereum с её смарт-контрактами и стандартом ERC-20, где за успешно выполненную задачи (task), согласно пунктам метода управления SCRAM будет присвоен «токен».

Автором доклада введена новая терминология тасккойн (taskcoin).

Таскойн (так же тасккойн, от анг taskcoin) – общее название криптовалют привязанных к рабочему времени либо исполнению определённой работы либо предоставлению услуги.

Пояснение: «Токены» приравнены к реальному, денежному, эквиваленту оплаты труда.

Список задач:

- оплата только за выполненное задание (задачу);
- гарантия получение оплаты труда;
- стабилизация активов;

- накопительная программа;

- доверие между двумя и более не доверяющими друг другу сторонами;

- защита от инфляции;

- гибкая управляемость налогообложением;

- открытая, прозрачная, понятная, доступная система оценивания.

Решение:

Например, работник за определённый объём выполненной работы получает токен, это может быть всё что угодно кассир в супермаркете, провёл 1000 ед товара получи токен, работник мебельной фабрики сдал 4 единицы изделия получил токен, программист выполнил задачу получил токен, в конце недели (Велико Британия) либо месяца по «токенам» выплачивается зарплата. Если работники находятся в разных странах, в разных валютных зонах «токены» гарантируют одинаковые условия труда и заработной платы вне зависимости от курса национальных валют.

Такая система гарантирует достойную оплату труда в странах со слабой экономикой в условиях сильной инфляции. Так же стабильность и управлением налогообложения в странах со стабильной экономикой и дифференцированной налоговой ставкой.

В идеале такая «токенизация» должна привести к росту активов компании и работника, если «токены» будут торговаться на бирже, то их стоимость будет расти и не сможет упасть ниже стоимости минимальной оплаты труда, то есть работник может продать «токены» и получить больший эквивалент в условных единицах, чем минимальная оплата труда. Если «токены» будут поддерживать платёжные системы, но без «обналичивания» можно будет обменять на товары и/или услуги. Таким образом может формироваться и портфель пенсионных накоплений, «токенов» разных компаний. По сути, токенизация - это процесс трансформации хранения и управления активом, при котором каждому активу ставится в соответствие цифровой двойник. Актив это и есть рабочие часы либо исполненные задания в компании, где он работал, которые в последствии работают на него.

Например, если в каком-то регионе существует оплата труда 10$ в час и анонсировано повышение оплаты до 12$ в час через месяц и на бирже существует предложение о продаже токенов по 11$, то инвестировав можно после повышения оплаты труда продать минимум по 12$.

Важно, чтобы в компании оставалось «замороженными» 51% токенов блокчейна, для гарантии неподверженности «атаки 51».

Так же важно, чтобы на реальных банковских счетах либо активов компании хватало, для погашения минимальной, актуальной стоимости таскойнов.

PROCESSING OF HIGH-DIMENSIONAL DATA SHEETS BY USING THE FUNCTION AND OPTIC-CONTROL TRANSPARANT

LysenkoH. L., KuzmenkoL.V.
Supervisor – Ph.D., assistant professor Lysenko H. L.
Vinnytsia National Technical University
(21021, Vinnitsa, st.Khmelnytsky highway, 95, Department of Laser and Optoelectronic Technology, tel.0432 598-450)
e-mail: kuzmenko600@gmail.com

Specialized computing systems (CS) are systems that are capable of performing complex operations with large-scale data, which are fed into arrays. In order to ensure the proper speed of operations in the specialized CS, it is necessary to create for them the possibility of parallel input, processing and output data. This can be done by using parallel methods of input, processing and output for specialized operating systems. The main ones are methods based on multi-tire buses, based on the parallel use of the frequency set and on the basis of controlled banners.

Optically controlled transparent (OCTs) represent a thin plate of electro-optical material and a conductive layer of semiconductor applied thereon. On both sides, this plate has two transparent electrodes.

For fast data processing, it is proposed to use optically controlled transparant using blockchain technology, that is, the creation of a hash of functions, that is, places.

Imagine this method to formulate a large-sized array of data, that is, matrix. We construct each matrix of cells in the code using the hashing function. To get the final result, we use the algorithm to add all values and get the result. This technology provides greater data processing speeds, and it works in the mode of parallel data input/output.

To use conventional banking as an analogy, the blockchain is like a full history of a financial institution's transactions, and each block is like an individual bank statement. But because it's a distributed database system, serving as an open electronic ledger, a blockchain can simplify business operations for all parties. For these reasons, the technology is attracting not only financial institutions and stock exchanges, but many others in the fields of music, diamonds, insurance, and Internet of Things (IOT) devices. Advocates have also suggested that this kind of electronic ledger system could be usefully applied to voting systems, weapon or vehicle registrations by state governments, medical records, or even to confirm ownership of antiquities or artwork.

Given the potential of this distributed ledger technology (DLT) to simplify current business operations, new models based on blockchain have already begun to replace the expensive and inefficient accounting and payment networks of the financial industry.

While banks were initially hesitant to explore these technologies because of their concerns about potential fraud, they have started looking into how the blockchain might provide generous cost savings by allowing back-office settlement systems to process trades, transfers and other transactions much faster.

Hashing is the process of converting an array of input data of arbitrary length into a (initial) bit string of fixed length. For example, a hash function can take a string with any number of characters (one letter or whole literary work), and at the output receive a string with a strictly defined number of characters.

In this paper, the main characteristics of the blockchain technology and the hashing of the function are analyzed. It was characterized that one of the main functions of the blockchain is its parallel processing and data analysis. In order to improve the productivity and speed analysis and data processing, it was suggested to use optically controlled banners, and to use hashing when working with large amounts of data. Further work will be aimed at improving the previously described functions, using a specialized blockchain based computing system using optically controlled banners.

To date, we have received the following data: for 512-bit units, the data processing time is 0.325ns, and the construction of hash functions according to 512-bit blocks is 181,174ns.

References:

1. Lysenko G. L., Tarnovsky M. G., Kuzmenko LV Currenttrendsinsolvingproblemsofdetectingandrecognizingobjectsonimages // Opto-electronicinformationalandenergetictechnologies. - 2017. - Vol. 33. - No. 1. - P. 18-23.
2. Quantum transducers on optoelectronic logic-time media for eye-processor processingImages: [Monograph] / VP Kozhemyako, T.B. Martynyuk, OI Suprigan, D.I. Klimkina - Vinnytsya: UNIVERSUM-Vinnytsia 2007. - 126 p. - ISBN 978-966-641-219-8
3. Image video-computer of eye-processor type: [Monograph] / VP Kozhemyako, G.L. Lysenko, AA Spring, AV Every one - Vinnytsya: UNIVERSUM-Vinnytsia, 2008. - 215s. - ISBN 978-966-641-261-7.
4. Roger Wattenhofer The Science of the Blockchain / Roger Wattenhofer – K. : Information technologies, 2016 – C. 94 – 120.

ВИКОРИСТАННЯ АПАРАТУ ЙМОВІРНІСНИХ P-P ГРАФІКІВ ДЛЯ ДОСЛІДЖЕННЯ РОЗПОДІЛУ ДКП КОЕФІЦІЄНТІВ JPEG ЗОБРАЖЕНЬ

Куріний А.А.
Науковий керівник – ст. викл. Федоров О.В.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки, 14, каф. інформаційно-мережної інженерії)
тел. (095)418-74-74, e-mail: artem.kurinyi@nure.ua

Digital technology allow people to receive and process enormous general information and securely store it. At present, one of the most important tasks is the creation of compression methods, the use of which allows improving the characteristics of the system of transmission, processing and data registration. The purpose of this work is to study the distribution of DCT of coefficients of JPEG images using a device of probabilistic P-P plots.

Використання цифрових технологій дозволяє людині отримувати та швидко обробляти великі обсяги інформації, компактно і надійно зберігати її, та швидко і легко отримувати доступ до неї. На даний час, однією з нагальних задач є створення методів компресії, застосування яких дозволило б поліпшити характеристики систем передачі, обробки та реєстрації зображень. Наявність адекватних ймовірнісних моделей ДКП коефіцієнтів дозволяє вирішувати такі задачі як сліпе оцінювання якості стиснених зображень або відео послідовностей (формати JPEG, V8, H265 та ін.), а також проводити оптимізацію параметрів алгоритмів компресії. Метою даної роботи є дослідження розподілу ДКП коефіцієнтів JPEG зображень із застосуванням апарату ймовірнісних *P-P* графіків [1].

Існує велике різноманіття статистичних моделей ДКП коефіцієнтів, що були запропоновані дослідниками. Найбільш вживаною моделлю залишається модель Лапласу $f_L(x) = (2\beta)^{-1} e^{-|x|/\beta}$. В окремих випадках також використовують узагальнений гаусів розподіл.

Модель Лапласу добре підходить для опису ДКП коефіцієнтів зображень, що мають у своєму складі достатню кількість дрібних деталей [2]. В свою чергу, ДКП коефіцієнти текстурних, і монотонних зображень можна описати двобічним гама розподілом $f_{\text{ГГ}}(x) = (2 \cdot \Gamma(\alpha) \cdot \beta^{\alpha})^{-1} \times$ $\times |x|^{\alpha-1} e^{-|x|/\beta}, \alpha > 0, \beta > 0$ [2]. Оскільки в JPEG файлах зберігаються тільки значення рівнів, отриманих в наслідок квантування ДКП коефіцієнтів, то доступні для аналізу дані мають дискретний характер. Отже класичні критерії узгодженості такі, як наприклад, критерій Колмогорова не підходять для перевірки гіпотези про вид розподілу. Критерій Пірсона χ^2 має малу наочність та залежність від розбиття на інтервали. Крім того, реальні дані можуть мати викиди, які неминуче призведуть до відхилення

гіпотези, що перевіряється. Однак на практиці наявність викидів незначною мірою впливає на точність прогнозів, що робляться із використанням певної статистичної моделі, якщо вона в цілому узгоджується з наявними даними.

Одним з можливих виходів з вказаної ситуації є використання апарату ймовірнісних графіків, а саме Q-Q та P-P. На відміну від Q-Q графіків, P-P графіки дозволяють також відобразити криві альтернативних розподілів. В нашому випадку на P-P графіку, що відповідає розподілу Лапласу, показати також криву двобічного гама розподілу.

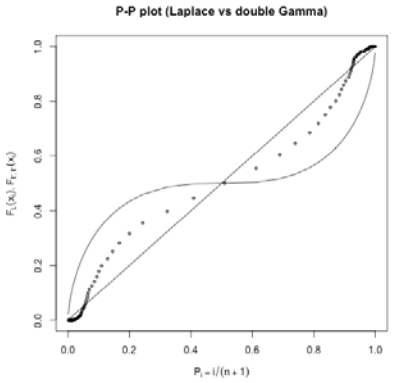


Рис. 1 – *P-P* графік «aurora» [3.1]

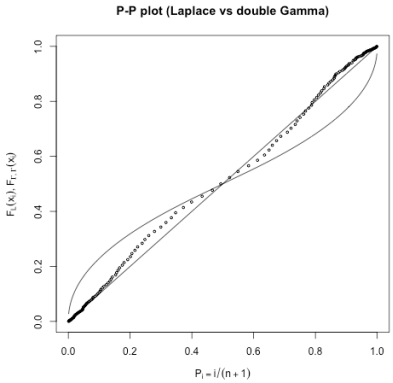


Рис. 2 – *P-P* графік «baboon» [4.1]

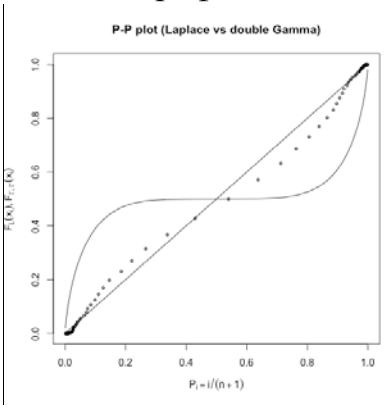


Рис. 3 – *P-P* графік «aurora» [4.1]

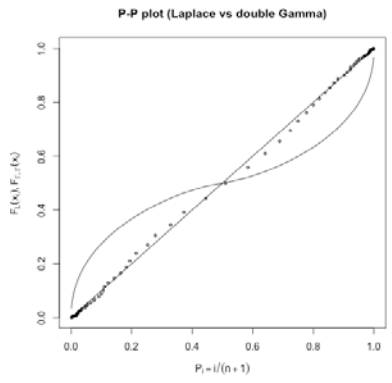


Рис. 4 – *P-P* графік «baboon» [8.1]

Класична модель Лапласа забезпечує відносно точний розподіл ДКП для тих зображень, що в більшості своїй складаються з областей багатих на дрібні деталі – зображення «baboon» (Рис. 2, Рис. 4). В той час, як для зображень, до складу яких входять суттєві області рівномірної яскравості (монотонних), модель у вигляді двобічного гама розподілу дозволяє отримати значно кращій результат – зображення «aurora» (Рис. 1, Рис. 3).

Перелік джерел:

1. Gan F.F., Koehler K.J. and Thompson J.C. Probability plots and distribution curves for assessing the fit of probability models // The American Statistician. – 1991. – Vol. 45, No. 1. – С. 14–21.

2. Родигін М.В., Федоров О.В. Врахування структурних властивостей зображення при оцінювані якості стиснених JPEG зображень // Східно-Європейський журнал передових технологій. – 2015. – Vol. 6/4, № 78.

ВЫБОР ПРЕДПОЧТИТЕЛЬНЫХ ПРОТОКОЛОВ МАРШРУТИЗАЦИИ АВТОНОМНЫХ СЕТЕЙ

Махник А. С.
Научный руководитель – к.т.н., доц. Скорик Ю.В.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Ленина,14, каф. Информационно-сетевой инженерии, тел. (057) 702-13-06)
e-mail: mak95@ukr.net

The analysis of routing protocols used in wireless sensor-actuator networks (WSAN) is carried out. The process of selecting an effective routing protocol for use in field sensor networks with the localization of elements by the method of analysis of hierarchies is considered. An energy-efficient routing protocol based on the location of the WSAN nodes has been identified.

За последние годы активное развитие беспроводных сенсорно-актуаторных сетей (БСАС) привело к появлению большого числа протоколов, алгоритмов и даже спецификаций, которые направлены на решение разного рода задач. Это и задачи эффективного сбора информации, и задачи поиска местоположения элементов сети, и задачи маршрутизации и многие другие. Такое многообразие протоколов повысило актуальность методов, с помощью которых можно выбрать из них наиболее эффективные для конкретного решения [1, 2].

БСАС эффективно используются для решения прикладных задач распределенного сбора информации о контролируемом параметре в сетях мониторинга и контроля. Такие сети обычно гомогенные, самоорганизующиеся, одноранговые, с ячеистой топологией, узлы имеют автономный источник питания и способны к ретрансляции информации. Автономный источник питания в виде батареи накладывает жесткие ограничения по энергоэффективности на все алгоритмы, применяемые в сенсорных сетях. Поэтому для БСАС актуальны следующие решения задач маршрутизации [3, 4]:

1. Задача поиска оптимальных маршрутов. При чем оптимальным считается маршрут доставки информации от отправителя до получателя, у которого суммарные затраты ресурсов (например, заряд батареи) входящих в него узлов минимальны.

2. Задача маршрутизации с обеспечение максимального времени жизни сети. Под временем жизни понимается срок эксплуатации сети до выхода из строя некоторого количества узлов из-за истощения заряда батарей, когда связность сети будет нарушена и информация не сможет достигнуть базовой станции (БС).

Исходя из этих двух критериев в статье рассмотрено применение метода анализа иерархий и метода экспертного оценивания для выбора протоколов маршрутизации для полевой БСАС с известным положением

элементов сети. Для выбора взяты следующие протоколы маршрутизации: SPIN, Directed Diffusion, Rumor Routing, LEACH, TEEN, PEGASIS, SOP, GAF, GEAR, SAR, SPEED [3, 4].

Метод анализа иерархий (МАИ) состоит в декомпозиции проблемы выбора единственного проектного варианта некоторой системы на простые составляющие части и получении суждений экспертов по парным сравнениям различных элементов проблемы выбора [1,2]. Принцип сравнительных суждений экспертов в МАИ состоит в том, что объекты проблемы выбора сравниваются экспертами попарно по важности. Попарно сравниваются важности разных вариантов систем и разных показателей качества. Результаты парных сравнений элементов приводятся к матричной форме. В результате обработки полученных численных данных суждений экспертов согласно определенной математической процедуры получают компоненты глобального вектора приоритетов, которые характеризуют приоритетность выбора вариантов проектируемой системы и определяют выбор единственного проектного варианта системы из заданного множества вариантов.

Методы экспертного оценивания – это методы организации работы со специалистами – экспертами и обработки мнений экспертов, выраженных в количественной и/или качественной форме с целью подготовки информации для принятия решений лицами, принимающимим решение. Определить необходимый численный состав экспертной группы очень важно. При недостаточном числе экспертов результаты экспертизы не будут надежными.

Применение метода анализа иерархий и метода экспертного оценивания для выбора протоколов маршрутизации показал возможность решить задачу выбора, используя данные от многих экспертов и строгий математический аппарат. На основе анализа предпочтительных протоколов маршрутизации получен результат выбора оптимального протокола для полевой беспроводной сенсорно-актуаторной сети с локализацией элементов.

Список використаних джерел

1. Bezruk V., Zelenin A., Vlasova V., Skorik J., Koltun Y. Select preferred of wireless sensor and actuator network // Eastern European Journal of Enterprise Technologies, 1/9 (79). – 2016. – P.4-9.

2. Безрук В.М., Скорик Ю.В. Применение метода анализа иерархий при выборе средств телекоммуникаций с учетом совокупности показателей качества // Радиоэлектроника и информатика. – Харьков: ХНУРЭ. – 2013. – С. 24-29.

3. Безрук В.М., Скорик Ю.В. Выбор оптимальных речевых кодеков методами экспертного оценивания // Восточно-Европейский журнал передовых технологий. – 2012. – 3/2 (57). – С. 19 – 24.

ОСОБЛИВОСТІ ВИКОРИСТАННЯ ТЕОРІЇ МЕРЕЖ МАСОВОГО ОБСЛУГОВУВАННЯ ДЛЯ МОДЕЛЮВАННЯ РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Морковін Є.О., Морковін О.О.
Науковий керівник – д.т.н., доц. Пустовойтов П.Є.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. IMI, тел. (057)702-14-29)
e-mail: yevhen.morkovin@nure.ua

Particularities of the use to theories of the networks of mass service for modeling of the portioned information systems. The processes of functioning of the real distributed information systems can not be described in detail due to the significant complexity of such systems. The model of the system should be on the one hand idle, and on the other - take into account the numerous features inherent in real systems.

Процеси функціонування реальних розподілених інформаційних систем (РІС) неможливо описати детально через істотну складності таких систем. Модель системи повинна бути з одного боку простою, а з іншого - враховувати численні особливості, властиві реальним системам. За своєю природою РІС відносяться до розряду складних технічних систем з дискретним характером функціонування і випадковим характером протікання процесів формування, обробки і передачі даних [1]. Тому для їх моделювання широко застосовуються аналітичні, імітаційні і комбіновані методи теорії систем масового обслуговування (СМО) з використанням мереж масового обслуговування [1,2]. В їх основу повинні бути покладені принципи, що поєднують системний підхід, ієрархічне багаторівневе моделювання і множинність моделей. Завдяки цьому вдасться забезпечити коректність і достовірність результатів моделювання, а в кінцевому підсумку проектування систем.

Подання схеми у вигляді графовій моделі мережі СМО [2], що включає для простоти розгляду три сервера обробки (СО), один сервер ініціалізації (СІ) і один сервер баз даних (СБД) наведено на рис.1.

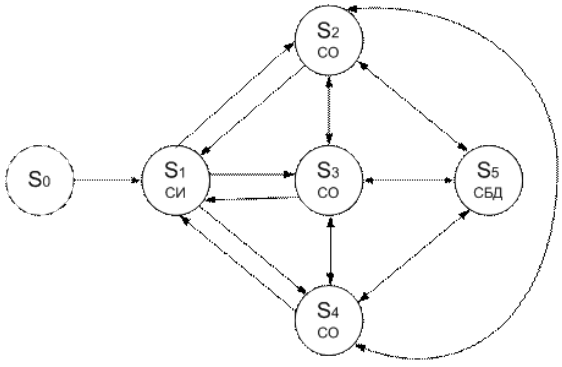


Рисунок 1 -Графові уявлення досліджуваної РІС

В якості базових моделей системи з пріоритетами використовуємо одноканальні або багатоканальні СМО з однорідним або неоднорідним потоками заявок. На їх основі побудуємо складну модель локального рівня (рис.1).

Розрахунок характеристик моделі будемо виробляти з використанням аналітичних залежностей, які враховують неоднорідність потоку заявок. Зокрема, середній час очікування заявок класу визначимо за формулою (1).

$$\omega_k^{СП} = \frac{\sum_{i=1}^{H}(2-q_{ki})\cdot(1+q_{ki})\cdot\lambda_i\cdot b_i^2\cdot(1+\nu_i^2)}{(2-\sum_{i=1}^{H}q_{ik}\cdot(3-q_{ik})\cdot\rho_i)\cdot(2-\sum_{i=1}^{H}(1-q_{ki})\cdot(2-q_{ki})\cdot\rho_i)} + \frac{b_k\cdot\sum_{i=1}^{H}q_{ik}\cdot(q_{ik}-1)\cdot\rho_i}{2-\sum_{i=1}^{H}q_{ik}\cdot(q_{ik}-1)\cdot\rho_i} \qquad (1)$$

де $\rho_i = \lambda_i \cdot b_i$ - завантаження, створювана заявками класу i, q_{ik}- елементи матриці пріоритетів ($i,k = 1..H$),які беруть значення: “0”, якщо заявка класу i не має пріоритету по відношенню до заявок класу k; “1”, якщо пріоритет відносний і “2”, якщо пріоритет абсолютний.

Середній час перебування запиту в системі (очікування і обробка) визначається середній затримкою його перебування в черзі і часом обслуговування в i-й СМО, і для багатоканальної СМО, яким є все СМО мережі, за винятком віртуальної СМО (джерела заявок) S_0 становить(3).

$$u_k = \omega_k + b_k \qquad (3)$$

Середнє число запитів, які перебувають у стані очікування (l_k)(4)

$$l_k = \lambda_k \cdot \omega_k \qquad (4)$$

Завдяки аналітичному моделюванню, проведеним на етапі проектування РІС, стає можливим прогнозувати поведінку системи, усувати "вузькі" місця і підвищувати ефективність функціонування в цілому.

Перелік посилань:

1. Л. Клейнрок «Теория массового обслуживания», М.: «Машиностроение», 1979г., 432 с.
2. Л. Клейнрок «Вычислительные системы с очередями», М.: «Мир», 1979г., 600 с.

ВИЗНАЧЕННЯ ЗАГАЛЬНИХ ПРИНЦИПІВ ОРГАНІЗАЦІЇ НАДІЙНОЇ БЕЗДРОТОВОЇ СЕНСОРНОЇ МЕРЕЖІ

Морковін О.О., Морковін Є.О.
Науковий керівник – д.т.н., доц. Пустовойтов П.Є.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. IMI, тел. (057)702-14-29)
e-mail: oleksandr.morkovin@nure.ua

The review of the basic principles of building a robust wireless sensor network, through an approach to the assessment of reliability based on the representation of wireless sensor network as markovski process and involves the use of mathematical models of reliability of data transmission between two nodes wsn, which, in turn, is a composition models the reliability of the nodes, the communication between them and the mechanism of their access to the environment.

Бездротові сенсорні мережі (БСМ) представляють собою локальні обчислювальні мережі, призначені для вирішення завдань моніторингу, управління ресурсами і процесами.

БСМ складаються з мініатюрних обчислювальних пристроїв - вузлів, забезпечених сенсорами (датчиками температури, тиску, освітленості, рівня вібрації, розташування і т.п.), прийомопередавачами сигналів, які працюють в заданому радіодіапазоні, і автономним джерелом живлення. Виділяють кілька різних типів вузлів: кінцеві пристрої (КП), оснащуються сенсорами і здійснюють вимірювання, маршрутизатори, передають інформаційні повідомлення від кінцевих пристроїв, координатор, який здійснює управління БСМ, а також шлюзи і мости, що зв'язують БСМ з іншими мережами.

Такі вузли, об'єднані в мережу, утворюють територіально-розподілену самоорганізуючу систему збору, обробки і передачі інформації і знаходять все більше широке застосування в таких областях, як:

- своєчасне виявлення можливих відмов виконавчих механізмів по контролю таких параметрів, як вібрація, температура, тиск і т. п .;
- контроль доступу в режимі реального часу до віддалених систем об'єкта моніторингу;
- автоматизація інспекції та технічного обслуговування промислових активів;
- енерго- та ресурсозберігаючі технології;
- контроль екологічних параметрів навколишнього середовища.

Найбільшого поширення останнім часом отримали БСМ, параметри яких регламентуються стандартом IEEE 802.15.4, а також специфікацією стека протоколів ZigBee. Далі будемо вести мову саме про такі мережі.

Технології побудови БСМ визначають їх переваги перед іншими рішеннями в області моніторингу: автономність вузлів, можливість їх розміщення в важкодоступних місцях, мале енергоспоживання, здатність до самоорганізації.

До недоліків БСМ можна віднести їх меншу надійність, під якою розуміється ймовірність безпомилкової і своєчасної доставки результатів вимірювань на мережеві шлюзи для подальшої обробки.

Надійність БСМ визначається багатьма факторами, найбільш суттєвими з яких є:

- надійність апаратного і програмного забезпечення вузлів;
- область розгортання мережі;
- взаємне розташування вузлів;
- період регламентного обслуговування мережі;
- інтенсивність збору і передачі інформації КУ;
- розмір переданих пакетів інформації.

Слід зазначити, що в даний час дослідження в області БСМ реалізуються в основному комерційними організаціями і носять приватний характер.

У зв'язку з особливостями експлуатації БСМ, мають місце втрати пакетів через наявність шумів, викликаних як іншими пристроями в конкуруючому діапазоні, так і наявністю власних ехосигналів. Імовірність успішної передачі повідомлення довжиною L_p байт от і-го вузла до j-го можна визначити із співвідношення

$P_{c_{ij}} = \left(P_{s_{ij}}\right)^{2L_p}$, де

$P_{s_{ij}}$ - імовірність безпомилкового прийому символу даних.

Залежність$P_{s_{ij}}$ від імовірності бітової помилки може бути отримана шляхом інтерполяції розрахункових значень для діапазону частот в 2.45ГГц, де використовується надлишкове кодування у відповідності із стандартом IEEE 802.15.4

Підхід до оцінювання надійності заснований на поданні функціонування БСМ, як марковского процесу, і передбачає використання математичної моделі надійності передачі даних між двома вузлами БСМ, яка, в свою чергу, являє собою композицію моделей надійності вузлів, комунікацій між ними і механізму їх доступу до середовищі.

МОДЕЛЬ ДОСТУПУ ДО ХМАРНОЇ ІНФРАСТРУКТУРІ ТА АНАЛІЗ ЇЇ ІМОВІРНІСНО-ЧАСОВИХ ХАРАКТЕРИСТИК

Педан М.М.
Науковий керівник – к. т. н., доц. Колтун Ю.М.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. «Інформаційно-мережна інженерія», тел. (057) 702-14-29)
E-mail: pigan10.94@gmail.com

The given work is devoted to the implementation effective model of access to the cloud infrastructure hosted on the data center of the standard architecture, and the assessment its performance indicators based on the analysis probability-time characteristics. In particular, formulas have been obtained for analyzing such quality indicators as the probability of blocking a request and the average delay time in the provision of a cloud service, which will allow to estimate the delay in connecting users to virtual machines. A numerical analysis has been made of the dependence of some the characteristics of the given load and the parameters model of access to cloud infrastructure.

Концепція хмарних обчислень полягає в наданні кінцевим користувачам віддаленого динамічно масштабованого доступу до послуг, обчислювальних ресурсів і додатків (включаючи операційні системи і мережну інфраструктуру) через Інтернет. При цьому користувачі отримують необхідні обчислювальні потужності за запитом через Web-інтерфейс хмарних додатків, без занурення в особливості реалізації цих програм і деталі системного адміністрування [1]. У зв'язку з цим, актуальними задачами є реалізація ефективної моделі доступу до хмарної інфраструктурі і оцінка її показників якості роботи [2, 3]. Необхідною вимогою для задоволення показників якості моделі доступу до хмарної інфраструктурі, є оцінка продуктивності хмарних центрів обробки даних (ЦОД). Вибір показників продуктивності залежить від задач проведення конкретного дослідження [2].

У доповіді розглядається хмарна інфраструктура, що розміщена у ЦОД, характерними рисами якого, є використання типових серверів стандартної архітектури, систем зберігання з горизонтальною масштабованістю і широке застосування технологій віртуалізації ресурсів [2]. Запропонована модель доступу до неї, де враховані показники продуктивності, які описуються імовірнісно-часовими характеристиками (ІЧХ), такими як, імовірність блокування запиту і середній час затримки у разі надання хмарної послуги.

Модель складається з C віртуальних машин, кінцевого буфера об'ємом r і системи моніторингу (рис. 1) [3]. Передбачається, що вхідний потік запитів є пуасонівським з інтенсивністю λ, а час надання хмарної послуги розподілений по експоненціальному закону із середнім $1/\mu$. Запити обслуговуються за дисципліною FIFO (першим прийшов, першим пройшов

обслуговування). За відстеженням числа зайнятих віртуальних машин відповідає система моніторингу, при цьому здійснюється вплив і на буфер і на функціонування віртуальних машин.

Також у доповіді робиться оцінка показників якості роботи моделі на основі аналізу ІЧХ. Основними ІЧХ моделі є імовірність блокування запиту P на надання хмарної послуги, середній час затримки $\bar{\tau}_1$ в наданні послуги у зв'язку з функціонуванням системи моніторингу і сумарний середній час затримки $\bar{T}$, що складається з часу $\bar{\tau}_1$ та середнього часу очікування початку надання послуги:

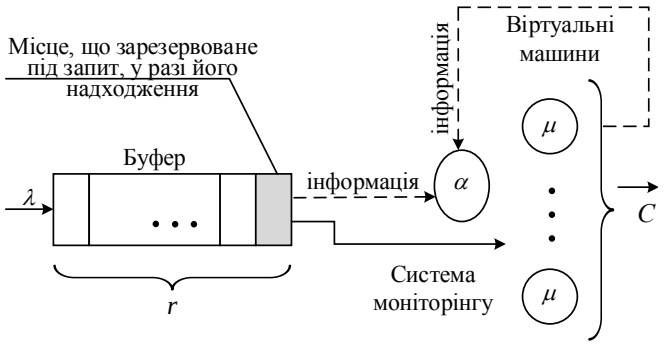


Рисунок 1 – Схема моделі доступу до хмарної інфраструктурі

$$P = p(R,0) + p(R,1),$$

$$\bar{\tau}_1 = \frac{\sum_{n=1}^{C-1} np(n,1) + C\sum_{n=C}^{R} p(n,1)}{\lambda(1-P)},$$

$$\bar{T} = \bar{\tau}_1 + \frac{\sum_{n=1}^{r} n(p(C+n,0) + p(C+n,1))}{\lambda(1-P)},$$

де n – число зафіксованих запитів у системі моніторингу;

$R = C + r$ – загальна сумарна кількість місць в системі.

Наданий варіант чисельного аналізу залежності деяких з характеристик від заданого навантаження і параметрів моделі доступу до хмарної інфраструктури.

Таким чином, реалізована в процесі досліджень модель доступу до хмарної інфраструктури дозволяє оцінити затримку в наданні хмарних послуг, що пов'язана з процесом моніторингу підключення користувачів до віртуальних машин і їх роботою щодо надання хмарних послуг.

Список джерел

1. Илья Клементьев Введение в облачные вычисления: учеб. курс [Електронний ресурс] / Клементьев Илья, Устинов Владимир – 2011. – Режим доступу до ресурсу: http://www.intuit.ru/studies/courses/673/529/info.

2. Ворожцов А.С., Тутова Н.В., Тутов А.В. Оценка производительности облачных центров обработки / А.С. Ворожцов, Н.В. Тутова, А.В. Тутов // T-Comm. – 2014. – №5. – С. 69 - 71

3. Гудкова И.А. Вероятностная модель для анализа задержки доступа к инфраструктуре облачных вычислений с системой мониторинга / И.А. Гудкова, Н.Д. Масловская // T-Comm. – 2014. – №6. – С. 13 - 15.

РАЗРАБОТКА СРЕДСТВ ПРОТИВОДЕЙСТВИЯ УПРАВЛЕНИЮ КВАДРОКОПТЕРОМ ДЛЯ ЗАЩИТЫ ЧАСТНОЙ ИНФОРМАЦИИ

Попаденко М.О., Коновалова К.Ю.
Научный руководитель – ас. Иваненко С.А.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, просп. Науки,14, каф. информационно-сетевой инженерии, тел. (057) 702-14-29)
e-mail: mariia.popadenko@nure.ua, ateryna.konovalova@nure.ua

Every year, automation increases its influence on our everyday life. There are many devices for development, training and other needs. Actually, quadcopter is the most functional and impressive invention. This device can do a variety of tasks. It has already found its widespread use in certain areas of human activity. Now such devices are available to every private person of ordinary consumers of electronics. Their cost has become acceptable, functional opportunities has grown, management became simpler. It comes as no surprise that such advantages, like a light weight, simple operation and availability, makes a certain threat to the privacy of people. In this project, in order to protect personal information, it is proposed to develop methods for counteracting these devices.

В наше время автоматизация увеличивает свое влияние на повседневную жизнь человека, появляется множество приборов для развития, обучения и других потребностей. Среди одних самых функциональных и впечатляющих является квадрокоптер.

Квадрокоптер (от англ. quadcopter — «вертолет с четырьмя винтами») — это беспилотный летательный аппарат с четырьмя пропеллерами, скорость вращения которых регулируется. Он оснащается стабилизирующими системами для обеспечения аэродинамической стойкости.

Концепция беспилотных летательных аппаратов достаточно быстро освоилась в кругах любителей радиоуправляемых устройств. Квадрокоптеры нашли широкое применение в различных областях, например: спасение людей, научные исследования, защита дикой природы и тому подобное. Но, к сожалению, квадрокоптер могут использовать не только во благо населения, но и для похищения конфиденциальной информации, наблюдения за людьми или незаконной съемки.

Для предотвращения подобных случаев были разработаны правовые нормы по использованию данного вида воздушной техники. К сожалению, органа, следящего за соблюдением этих норм, как такового, нет. Все это вызвало повышенный интерес к решениям, направленных на борьбу с подобного рода аппаратами.

В работе рассматриваются следующие методы противодействия квадрокоптерам, а именно: глушение, физическое противодействие, подмена GPS-координат, перехват управления.

Большое количество квадрокоптеров может руководствоваться с использованием технологии Wi-Fi. Поэтому в научной работе один из предоставленных методов использует именно особенности этой технологии, так как возможно выполнить противодействие управлению квадрокоптера. Главным элементом использования этого метода является Wi-Fi jammer (это устройство, которое предназначено для отключения беспроводных устройств от точки доступа)

Не все квадрокоптеры могут управляться с использованием Wi-Fi, поэтому в научной работе был рассмотрен еще один прибор, а именно генератор помех для GPS, который является более универсальным. При постановлении помех по этому каналу уязвимы все типы квадрокоптеров, которые управляются с помощью интеллектуальных режимов с использованием GPS. Исключением является только спортивные квадрокоптеры, которые недостаточно распространены. Для повышения качественных характеристик предложенных устройств была разработанная направленная антенна.

Список литературы:

- Поваляев Е., Хуторной С. Системы спутниковой навигации ГЛОНАСС и GPS //Ч. 3. Борьба с многолучевостью.-" Инженерная микроэлектроника". – 2002. – No. 2. – С. 23. - Кумисбек Г. М. Квадрокоптер-беспилотный летательный аппарат: возможности и технические свойства. Материалы научного семинара //Астана, ДШ. – 2013. - Демуренко К. А. Дроны-новая угроза с высоты //Алгоритм безопасности. – 2016. – No. 2. – С. 48.

ДИСТАНЦІЙНО КЕРОВАНИЙ РОБОТ-РОЗВІДНИК ІЗ СИСТЕМОЮ ЗБОРУ, ПЕРЕДАВАННЯ ТА ЗБЕРЕЖЕННЯ ВИМІРЮВАЛЬНОЇ ІНФОРМАЦІЇ

Пушкарьов В. В.
Науковий керівник: - к.т.н., доц. Бондарь Д. В., ст. викл. – Малінін О. П.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки, 14, каф. інформаційно-мережної інженерії, (057) 702-14-29)
e-mail: slavik5320xm@gmail.com, тел. 097-357-81-89

Topicality of the topic: In order to solve the security problem in emergencies, it is necessary to create more modern specialized technical equipment and equipment for intelligence and information gathering at a safe distance for staff. This could help to protect the personnel, fire and rescue equipment from the influence of dangerous factors of fire, explosion, gamma radiation, etc.

The purpose and tasks of the scientific work: to develop a telecommunication complex consisting of a mobile platform for intelligence and a server for data collection and analysis in emergencies.

Якість ліквідації аварій або надзвичайних ситуацій та безпека персоналу, що виконує ці роботи на пряму пов'язана з технічною оснащеністю та засобами попередження і локалізації аварії і залежать від неї. Основні втрати спостерігаються при виникненні складних аварій, де робота персоналу особливо ускладнена, де велика ймовірність впливу вторинних проявів небезпечних факторів. До таких ситуацій, наприклад, відносяться пожежі на складах боєприпасів, які є найбільш небезпечними, оскільки здатні завдати великої матеріальної шкоди та привести до людських жертв, аварії на підприємствах хімічної галузі, тощо Для вирішення проблеми безпеки при подібних ситуаціях виникає необхідність у створенні більш сучасних спеціальних технічних засобів і обладнання для проведення розвідки та збору інформації на безпечному для персоналу відстані. Це могло б сприяти захисту особового складу, пожежної та аварійно-рятувальної техніки від впливу на них небезпечних факторів пожежі, вибуху, гамма-випромінення і т.д.

У даній доповіді представлено телекомунікаційну систему, що складається з дистанційно керованого робота-розвідника із системою збору та подальшого збереження отриманих даних. Телекомунікаційний комплекс був розроблений для забезпечення безпеки при роботах в обмеженому просторі, місцях з обмеженим доступом або небезпечної для здоров'я і життя атмосферою. В тому числі, система може бути використана як робот радіаційної розвідки. Компактний робот розвідки здатний виконувати різні завдання: проводити вимірювання температури та вологості повітря, проводити аналіз атмосфери на наявність горючих і

токсичних газів. Місцезнаходження мобільної платформи можно відслідковувати за допомогою вбудованого в неї GPS-ресивера. Живлення платформи виконується літієвими акумуляторами великої ємності, що забезпечує роботу системи при максимальній потужності приємно-передаючих пристроїв до 5-6 годин. Дистанційне керування бездротова комунікація для обміну даними робота з сервером відбувається по радіоканалу за допомогою енергоефективних модулів NRF, які забезпечують дальністю зв'язку до 1000 метрів.

Головні переваги в порівнянні зі схожими системами:

- мобільний - транспортування робота можливо у невеликій сумці;
- компактний - робот розвідки здатний проникнути через отвір діаметром від 20 см.
- захищений – міцний та легкий корпус з текстоліта.
- маневрений - робот може обертатися на 360 ° навколо своєї осі.
- радіокерування - відсутність проводів і кабелів.
- легкість керування - обслуговуючий персонал робота-розвідника складається з однієї людини.

В доповіді було розглянуто телекомунікаційну систему, що складається з дистанційно керованого робота-розвідника із системою збору та подальшого збереження отриманих даних. Приведено характеристики використаних електронних модулів, датчиків, системи радіозв'язку сервера з рухомою платформою та програмні засоби організації сервера для збереження та подальшого аналізу отриманих даних.

Подальша модернізація системи передбачає встановлення більш енергоефективної системи електроживлення, та радіозв'язку між сервером та роботом. Встановлення більш потужних модулів зв'язку , наприклад, «LoRa» підвищить стабільність зв'язку, максимальну дальність зв'язку до декількох кілометрів, навіть, при відсутності прямої видимості між прийомною та передаючою сторонами. Також потрібно організувати захист даних, що передаються по бездротовій системі. Можна вдосконалити роботу системи визначення місця розташування робота за допомогою встановлення GPS-репітера.

Таким чином даний телекомунікаційний комплекс може бути застосований в реальних умовах при надзвичайних ситуаціях, а також для доступу до малодоступних приміщень, тощо.

Перелік джерел

1. Simple-SCADA [Електроний ресурс]: https://simple-scada.com
2. Контролери Atmega [Електроний ресурс]:http://avr.ru/docs/d-sheet/atmega
3. OPCserver [Електроний ресурс]: https://insat.ru/services/1
4. MySQLserver [Електроний ресурс]: https://www.mysql.com/services/

РАСПОЗНАВАНИЕ ЭМОЦИЙ ДИКТОРА ПО ЕГО ГОЛОСУ

Самочернов Н.Б.
Научный руководитель – к.т.н., доц. Омельченко С.В.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Науки,14, каф. Информационно-сетевой инженерии)
e-mail: nick.samochernov@gmail.com, тел. (068) 450-95-91

An algorithm for automatic emotion recognition from the speaker's voice has been developed. The classification efficiency for different acoustic features was estimated and a very small set of the most reliable characteristics was extracted in order to obtain a robust and quick emotion state classification. Using the classifier with quadratic kernel and this feature set provides the recognition accuracy of approximately 96 % between “anger” and “neutral” emotional states.

Key words: voice, emotions, emotional state, emotional speech.

Автоматическое распознавание эмоционального состояния окажется полезным в любой сфере человеческой деятельности, где требуется его оперативная оценка — в маркетинге, медицине, психологии, обеспечении безопасности и т. п.

Однако, проблема взаимосвязи эмоциональных состояний диктора с параметрами его голоса до сих пор полностью не решена. Основой алгоритма голосового анализа является модуль выделения информативных признаков речевого сигнала и классификатор, относящий звуковой фрагмент, согласно этим признакам, к тому либо иному эмоциональному классу. Соответственно, выделение новых, по возможности родственных человеческому восприятию, информативных признаков, а также поиск новых высокоэффективных техник классификации на текущий момент времени являются важнейшими задачами голосового распознавания эмоционального состояния. Чаще всего в целях дальнейшего анализа из аудио сигнала выделяют: различные параметры частоты основного тона и формант; кратковременную оценку мощности; темп речи (количество слов произносимых в единицу времени); контур основного тона.

На основе выделяемого набора информативных признаков строится классификатор, который обучается на предварительно подготовленном наборе звуковых фрагментов. Наиболее популярными техниками классификации являются следующие [1]: поиск ближайших соседей, метод опорных векторов, скрытые марковские модели, модель смеси нормальных распределений, модели на основе нечеткой логики, байесовские классификаторы максимума вероятности.

База включает 500 записей речи 10 дикторов (5 мужчин, 5 женщин), воспроизводящих набор дискретных эмоциональных состояний, называемых базовыми (гнев, раздражение, страх, радость, печаль, удивление и нейтральное состояние).

В качестве возможных информативных признаков был выделен ряд признаков: оценка мощности, частота основного тона (ЧОТ), асимметрия от медианы ЧОТ, линейные спектральные частоты, кепстральные коэффициенты, вычисленные по коэффициентам предсказания, статистики высшего порядка, энергетический оператор Тигера [2].

Количество записей в обучающей выборке при этом составляло 80 штук — 40 записей для нейтрального состояния, и 40 для состояния гнева. Тестирование алгоритма позволило выявить ряд информативных признаков, эффективность классификации эмоциональной речи по которым оказалась максимальной. Наиболее значимыми для принятия решения о принадлежности записи к классу нейтрального состояния и состояния гнева информативными признаками оказались частота основного тона, 2ой коэффициент линейных спектральных частот, вторая производная оценки мощности и эксцесс ошибки линейного предсказания.

Для выбранного набора параметров, оценки точности работы алгоритма классификации оказались следующими. Ошибка классификации в случае использования метода опорных векторов составила порядка 4 %. При применении модели смеси нормальных распределений соответствующее значение оказалось равным примерно 6 %.

Таким образом, использование выделенных информативных признаков позволило распознавать с точностью порядка 94–96 % в зависимости от используемого алгоритма классификации.

В состоянии гнева диктор издает звуки с более открытым речевым трактом, что приводит к возрастанию средней частоты первой форманты. В состоянии гнева существует влияние на характеристики частоты основного тона. Возрастает его медианное значение, скорость изменений, расширяется его диапазон. Так же, по отношению к ней, возрастают амплитуды второй и третьей формант, повышается неоднородность формантных контуров. Кроме частотных параметров голоса важную роль играют характеристики огибающей его энергии.

Увеличение числа распознаваемых эмоций, равно как и переход от модельных эмоциональных баз данных к реальным, необходимо ведет к возрастанию ошибки классификации. Точность распознавания одного из семи эмоциональных состояний эмоциональной речи порядка 89 % .

Список источников

1. Cornelius R. R. 1996. The Science of Emotion: Research and Tradition in the Psychology of Emotions.

2. Morrison D., Wang R., De Silva L. C. 2007. Ensemble Methods for Spoken Emotion Recognition in Call-Centres. Speech Communication, 4 : 98–112. Voice emotion classification: problems and solutions 195

ОСОБЛИВОСТІ АРХІТЕКТУРИ MESH- МЕРЕЖІ

Сірик А.В.
Научный руководитель – доц., к.т.н. Токарь Л.А.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Науки, 14, кафедра инфокоммуникационной инженерии, тел. +380990283022, e-mail: vulpesinculta22@gmail.com

The principle of construction of a Mesh network is considered. The peculiarity of such networks is self-organizing architecture, which makes it possible to use it in various fields. It is shown that this technology becomes especially necessary in the absence of wired infrastructure for connecting stations. And the use of special protocols allow each access point to create a table of network subscribers with control of the transport channel and support for dynamic routing of traffic with the best route between neighboring stations.

Системи на базі технології Mesh забезпечують високошвидкісну передачу цифрової інформації, відео-і мовний зв'язок, а також визначають місце розташування об'єктів.

Mesh-мережа – це багатокрокова мережа, пристрої якої (Mesh-станції, MP, Mesh-Points) володіють функціями маршрутизатора і здатні використовувати різні шляхи для пересилки пакету. Ця технологія стає особливо необхідною за відсутності провідної інфраструктури для з’єднання станцій. В цьому випадку пакети пересилаються від однієї Mesh-станції до іншої до досягнення шлюзу з провідною мережею.

Поняття Mesh визначає принцип побудови мережі, відмітною особливістю якої є самоорганізована архітектура, що реалізує можливості створення зон суцільного інформаційного покриття великої площі, масштабованість мережі у режимі самоорганізації, використання безпровідних транспортних каналів (backhaul) для зв'язку точок доступу в режимі «кожен з кожним» та стійкість мережі до втрати окремих елементів.

Особливістю Mesh-мереж є використання спеціальних протоколів, що дозволяють кожній точці доступу створювати таблиці абонентів мережі з контролем стану транспортного каналу і підтримкою динамічної маршрутизації трафіку з оптимальним маршрутом між сусідніми станціями. При відмові будь-якої з них відбувається автоматичне перенаправлення трафіку по іншому маршруту, що гарантує отримання трафіка адресату за мінімальний час. Завдяки своїм особливостям Mesh-мережі можуть використовуватись в різних сферах [1].

Основна відмінність Mesh-мережі від архітектури «крапка-багатокрапка» в тому, що якщо в останньому випадку абонентська станція (АС) може спілкуватися тільки з базовою станцією (БС), то в Mesh-мережі можлива взаємодія безпосередньо між АС.

Оскільки мережі стандарту IEEE 802.16 орієнтовані на роботу з широкими частотними каналами, Mesh-мережі увійшли до стандарту як необхідний інструмент побудови широкосмугової мережі, в якій трафік може передаватися по ланцюжку з декількох станцій, ліквідовуючи тим самим проблеми передачі за відсутності прямого бачення. Відповідно тому всі механізми управління, що у принципі дозволяють побудувати децентралізовану розподілену мережу, орієнтовані на деревовидну архітектуру, з виділеною базовою станцією і домінуючими потоками БС-АС.

В Mesh-мережі всі станції формально рівноправні. Проте, практично завжди обмін трафіку Mesh-мережі із зовнішнім оточенням відбувається через одну станцію. Така станція називається базовою станцією Mesh-мережі: саме на неї покладається частина необхідних для управління Mesh-мережею функцій. При цьому управління доступом може відбуватися або на основі механізму розподіленого управління, або централізованим способом під управлінням БС.

Базове поняття в Mesh-мережі – сусіди. Під сусідами певної станції розуміють всі станції, які можуть встановлювати з нею безпосереднє з'єднання. Всі вони утворюють сусідське оточення. Станції, що пов'язані із заданим вузлом через сусідську станцію, називають сусідами другого порядку. Можуть бути сусіди третього порядку та інші.

В Mesh-мережі немає поняття висхідних/низхідних каналів: весь обмін відбувається за допомогою кадрів. Станції передають повідомлення або у відведені їм тимчасові інтервали, або дістають доступ до каналів довільним чином.

Кожна станція має унікальну 48-розрядну MAC-адресу. Крім того, для ідентифікації усередині Mesh-мережі станціям присвоюється 16-розрядний мережний ідентифікатор. Кожна станція постійно зберігає список даних про всіх своїх сусідів (з вказівкою віддаленості, сектора для направленої антени, необхідної потужності передавача, затримки розповсюдження сигналу і т.і.) і транслює його в мережу із заданою періодичністю. На підставі цих списків від кожної станції відбувається управління мережею.

«Мережний вхід» - це інтервал, протягом якого нова станція може послати повідомлення (NENT) про свій намір підключитися до мережі. Перед цим вона повинна прийняти повідомлення про конфігурацію мережі, вибрати станцію для підключення, синхронізуватися з нею і лише потім відправляти запит. У відповідь станція може або відмовити в доступі або призначить новій станції мережний ідентифікатор, канал й часовий інтервал для проведення процедур аутентифікації.

Список источников:

1. Маккалоу, Джек. Секреты беспроводных технологий [Текст]: пер. с англ. – М.: НТ-Пресс, 2005, 404 с.

DESIGNING OPTIMUM ENTROPY CONSTRAINED QUANTIZERS FOR MEMORYLESS SOURCES

Stepanov O.O.
Scientific supervisor - senior lecturer Fedorov O.V.
Kharkiv National University of Radio Electronics
(61166, Kharkov, Nauky Ave. 14, dep. of Information and Network Engineering, tel. (057) 702-14-29)
e-mail: oleksandr.stepanov@nure.ua

This note aims at discovering the applicability of geometric programming to obtain optimal quantizers for memoryless sources. In what follows we stick to Forwardin & Modestino's notation and consider the problem of constrained optimization, namely, the problem of constructing an N-level quantizer subject to an entropy constraint.

Sampling and quantization are two major operations performed when digitizing analog signals. To avoid aliasing, one should select the sampling frequency so as to satisfy the sampling theorem, namely, prior to the sampling the input signal must be bandlimited with the highest frequency being twice as small as the sampling frequency. Unfortunately there is no straightforward solution for the quantization stage, the result depends on the probability distribution of the signal to quantize. Moreover, different approaches to the problem of constructing an optimal quantizer are possible: (i) unconstrained optimization and (ii) constrained optimization when we limit the entropy of the output sequence. For the case of unconstrained optimization, there exist well developed techniques, both for scalar and vector quantization [1].

Entropy constrained quantization relies on the Rate-Distortion theory [2] and underlies all the modern algorithms of lossy compression of multimedia data. For the entropy constrained quantization, we also have a bunch of algorithms, which were proven to work well [3]. However, efficient algorithms exist only for memoryless probability distributions, namely, for exponential and double exponential ones [4]. That is it, the objective of this paper is to develop a solution to the problem of designing entropy constrained quantizers based on principles of geometric programming [5].

In what follows we are going to use the Farvardin & Modestino notation [3]. That is it, $\{X_t\}$ is for a discrete-time memoryless stationary process and $X_t \sim f(x)$, where $f(x)$ is a probability density function. Under the N-level quantizer we will understand a function $q_N(\cdot)$ which maps $\{X_t\}$ onto one of $\{Q_n\}_{n=1}^{N}$ levels. In terms of threshold values $\{T_n\}_{n=1}^{N-1}$, $q_N(\cdot)$ can be defined as:

$$q_N(x) = \sum_{i=1}^{N} Q_l I_l(x),$$

where $I_l(x)$ equals 1 if $x \in (T_{l-1}, T_l]$ and 0 otherwise.

To assess the total alteration of $\{X_t\}$ introduced by the N-level quantizer, an average distortion function is used:

$$D_N(\vec{T},\vec{Q}) = \sum_{i=1}^{N}\int_{-\infty}^{\infty} d(x,Q_l) I_l(x) f(x)dx,$$

where $d(\cdot,\cdot)$ is the non-negative measure of distortion and $\vec{T} = [T_1, T_2, ..., T_{N-1}]^T$ $\vec{Q} = [Q_1, Q_2, ..., Q_N]^T$.

The entropy constrained scalar quantizer is said to be [3]:

$$\begin{gathered} D_N(\vec{T},\vec{Q}) \to \min \\ \text{subject to} \quad H_N(\vec{T}) = -\sum_{l=1}^{N} P_l \log_2 P_l \le H_0 \end{gathered} \tag{1}$$

where $H_N(\vec{T})$ is the entropy of the quantizer output and $P_l = \int_{-\infty}^{\infty} f(x) I_l(x) dx$.

To solve the problem (2) we a going to use the methods of Lagrange multipliers, which leads to the system of $2N+1$ equations, namely

$$\begin{cases} \frac{\partial}{\partial T_l}\int_{T_{l-1}}^{T_l} d(x,Q_l) f(x)dx - \frac{\partial}{\partial T_l}(P_l \log_2 P_l) = 0, \\ \frac{\partial}{\partial Q_l}\int_{T_{l-1}}^{T_l} d(x,Q_l) f(x)dx = 0, \\ -\sum_{l=1}^{N} P_l \log_2 P_l - H_0 = 0. \end{cases} \tag{2}$$

In case if the PDF of $\{X_t\}$ is exponential, i.e. $f(x) = \beta^{-1}\exp(-x/\beta)$ and the distortion measure $d(\cdot,\cdot)$ is mean squared error, the system (2) becomes

$$\begin{cases} \beta^{-1} e^{-T_l/\beta}[(T_l - Q_l)^2 - \lambda \log_2(e^{1-T_{l-1}/\beta} - e^{1-T_l/\beta})] = 0, \\ 2[e^{-T_{l-1}/\beta}(T_{l-1} - Q_l + \beta) - e^{-T_l/\beta}(T_l - Q_l + \beta)] = 0, \\ -\sum_{l=1}^{N}(e^{-T_{l-1}/\beta} - e^{-T_l/\beta}) \log_2(e^{-T_{l-1}/\beta} - e^{-T_l/\beta}) - H_0 = 0. \end{cases} \tag{3}$$

Now, eliminating λ and expressing Q_l in terms of T_l, we reduce the system (2), composed of $2N+1$ equations, to a system of $N+1$ equations, which is solvable within the framework of geometric programming.

References

1. R. M. Gray and D. L. Neuhoff. Quantization. *IEEE Transactions on Information Theory*, 44(6):2325–2383, Oct 1998.

2. L. D. Davisson. Rate-distortion theory and application. *Proceedings of the IEEE*, 60(7):800–808, 1972.

3. N. Farvardin and J. Modestino. Optimum quantizer performance for a class of non-gaussian memoryless sources. *IEEE Transactions on Information Theory*, 30(3):485–497, May 1984.

4. G. J. Sullivan. Efficient scalar quantization of exponential and laplacian random variables. *IEEE Transactions on Information Theory*, 42(5):1365– 1374, Sep 1996.

5. S. Boyd, S.-J. Kim, L. Vandenberghe, and A. Hassibi. A tutorial on geometric programming. *Optimization and engineering*, 8(1):67, 2007.

АВТОРИЗАЦІЯ НА САЙТІ ЗА ДОПОМОГОЮ RFID - РІДЕРА

Ходаківський М.А.
Науковий керівник: - к.т.н., доц. Бондарь Д. В., ст. викл. – Малінін О. П.
Харківський національний університет радіоелектроніки
(61186, Харків, просп. Науки, 14, каф. інформаційно-мережної інженерії, (057) 702-14-29)
e-mail: mykola.khodakivskyi@nure.ua тел. 098-886-12-65

RFID systems are used in a variety of cases where operational and precise control, tracking, and taking into account the numerous displacements of various object is required.

In this paper, an authorization system using RFID access is presented to you. The system may be used for authorization on a personal computer, as well as authorize on any site without the use of input devices. The power supply of the platform is carried out with the help of any power supply in the range of voltage from 5 to 9 volts, or simply submerge the USB connector.

RFID - системи застосовуються в різноманітних випадках, коли потрібен оперативний і точний контроль, відстеження і урахування численних переміщень різноманітних об'єктів.

У даній роботі представлено систему авторизації за допомогою RFID доступу. Систему можливо використовувати для авторизації на персональному комп’ютері, а також авторизуватися на будь-якому сайті без використання пристроїв вводу інформації . Живлення платформи виконується за допомогою будь-якого джерела постійного струму живлення в діапазоні напруги від 5 до 9 вольта.

Головні переваги в порівнянні зі схожими системами:

- Адаптованість її можна використовувати не тільки для виконання певної задачі, а для виконання декількох одночасно, наприклад розблокування комп’ютера та авторизація на сайті;
- Легкість встановлення на будь-яку машину.

Система може застосовуватися як:

- Електронний контроль за доступом і переміщеннями персоналу на території підприємств;
- Керування виробництвом, товарними і митними складами (особливо значними), магазинами, видачею і переміщенням товарів і матеріальних цінностей;
- Автоматичний збір даних і при необхідності нарахування оплати на залізницях, платних автомобільних дорогах, на вантажних станціях і терміналах;
- Контроль, планування і керування рухом, інтенсивністю графіка і вибором оптимальних маршрутів;
- Громадський транспорт — керування рухом, оплата проїзду й оптимізація пасажиропотоків.

Структура системи доступу складається з:

- Плати Arduino Leonardo;
- RFID – рідера RC522;
- Контролер для керування (Atmega3204);
- RFID – мітки, або будь-яка інша картка;

На сьогоднішній день користь, яку приносить радіочастотна ідентифікація важко переоцінити велика кількість різноманітних операцій виконується за допомогою RFID – технології, на підприємстві, складі, або бібліотеці, тощо майже всюди можна знайти використання RFID - технології. В моєму проекті я розробив систему авторизації на будь-які ресурси інтернет, це може бути досить зручно, коли треба швидко, і точно увійти в якусь систему . Система також дозволяє авторизуватися в операційній системі. В системі використовується база даних, що також дає змогу моніторити коли було включення системи, або авторизація.

Перелік джерел

1.Максим Власов. RFID: 1 технологія - 1000 рішень: Практичні приклади використання RFID в різних областях. - М .: Паблішер, 2014. - 218 с. - ISBN 978-5-9614-4879-5;

2.Сандип Лахірі. RFID. Керівництво по впровадженню = The RFID Sourcebook / Дудників С .. - М .: Кудіц-Пресс, 2007. - 312 с. - ISBN 5-91136-025-X;

3.Маніш Бхуптані, Шахрам Морадпур. RFID-технології на службі вашого бізнесу = RFID Field Guide: Deploying Radio Frequency Identification Systems / Троїцький Н .. - М .: «Альпіна Паблішер», 2007. - 290 с. - ISBN 5-9614-0421-8;

4.Т. Шарфельд (до Додатків І. Девіль, Ж. Дамур, Н. Чаркані, С. Корнєєва та А. Гулар). Системи RFID низької вартості / С. Корнєєв. - М., 2006;

5.Клаус Фінкенцеллер. Довідник по RFID. - М .: Видавничий дім «Додека-XXI», 2008. - 496 с. - ISBN 978-5-94120-151-8.

ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНІ ТЕХНОЛОГІЇ, МЕТРОЛОГІЧНЕ ЗАБЕЗПЕЧЕННЯ, СТАНДАРТИЗАЦІЯ І СЕРТИФІКАЦІЯ

ТОЧНІСТЬ ТА ПОХИБКА ВИЗНАЧЕННЯ МІСЦЕПОЛОЖЕННЯ РУХОМОГО ЗАЛІЗНИЧНОГО ТРАНСПОРТУ І ВПЛИВ ЗОВНІШНІХ УМОВ

Аль РавашдехЛейт Ахмед Мустафа
Науковий керівник д.т.н. проф. Руженцев І.В.
Харківськийнаціональнийуніверситетрадіоелектроніки
61166, Харків, просп. Науки,14, каф. МТЕ, тел. (057) 702-13-31
e-mail: d_mme@nure.ua

The urgency of the chosen topic is determined by the need for the development and application of systems for locating mobile rail transport for the purpose of managing mobile objects of railway transport.

Thepurposeoftheworkistoformulateandsolvetheproblemofimprovingthetransportationprocessinordertoincreasetheefficiencyofitsoperationbymeansofthesystemoflocatingtherailwayrollingstock.

Theresultsoftheworkaredevelopmentof a productionprogramfordeterminingthelocationofmobilerailtransport.

Моніторинг парку рухомого складу і управління ним являють собою комплекс технічних і організаційних заходів по контролю за переміщенням рухомого складу для організація обліку витрат, попередження крадіжок, забезпечення користувачів послугами залізниці актуальною інформацією про можливі затримки прибуття. Супутникова навігація застосовується також для дослідження стану залізничного полотна (наприклад, геометрії колії) для гарантування безпечного проходження складу [1].

На сьогоднішній день існують різні варіанти організації системи визначення місця розташування рухомої одиниці на базі ГНСС, тому проведення аналізу можливих рішень є необхідним етапом для вибору конкретного підходу при реалізації системи визначення місця розташування рухомої одиниці для напрямків, представлених на рисунку. Перш за все для цих напрямків необхідно сформулювати вимоги, які повинні бути пред'явлені до системи визначення місця розташування рухомої одиниці щодо характеристик навігаційного сервісу, що визначають його якість, а саме:

– горизонтальна точність положення – величина, що визначає невідповідність виміряного розташування в заданий момент часу істинному на горизонтальній площині;

– межа тривоги для помилки по горизонталі (МТГ) – максимальна допустима помилка в обчислення місця розташування;

– час до тривоги (ЧДТ) – час, протягом якого користувач повинен бути проінформований, якщо перевищено межу тривоги для помилки по горизонталі (МТГ);

– ризик цілісності (РЦ) – визначає ймовірність того, що користувач не буде проінформований про перевищення допустимої величини помилки

протягом час до тривоги. Ризик цілісності визначено для найбільш критичних режимів функціонування і тому вимірюється в одиниці, поділеній на 150 с (1/150 с);

– безперервність (БП) – характеризує здатність навігаційної системи гарантовано надавати сервіс, коли це дійсно необхідно (визначено для найбільш критичних стадій функціонування);

– доступність (ДП) – відсоток часу від усього терміну функціонування системи, коли сервіс наданий відповідно до необхідних точності, цілісності і безперервності в будь-якій точці зони покриття.

Так як мова йде про можливості використання супутникової технології в забезпеченні безпеки руху, то відсутність підтвердження про МТГ протягом ЧДТ можна розцінювати як небезпечну відмову. Тоді значення РЦ, що задовольняє SIL4, може бути виражено наступним чином:

$$\text{РЦ} = P_{oo} \cdot \frac{150\text{с}}{150\text{с}}$$

Отже, необхідне значення:

Таким чином, можна визначити, що необхідний рівень РЦ для залізничної галузі повинен бути приблизно менше ніж $10^{-10} \frac{1}{150\text{с}}$.

Інтегруюча система позиціонування виробляє обробку даних супутникової навігації і додаткових вимірювальних перетворювачів (датчиків) із застосуванням алгоритму фільтрації (наприклад, фільтр Калмана).

Точність інтегруючої системи позиціонування при поєднанні даних від систем GPS і Глонасс та інерційних датчиків може досягти 3 мс з ймовірністю 95 % (проект APOLO).

Список джерел

1. Розенберг И.Н. Применение технологий спутниковой навигации, космического дистанционного зондирования и спутниковой связи в интересах железнодорожного транспорта: монография / И.Н. Розенберг, Н.В. Сазонов, М.М. Железнов, А.С. Василейский. – М.: ИКИ РАН, 2008 – 47 с.

КАЛІБРУВАННЯ ТЕРМОМЕТРА

Брікман А.І.
Науковий керівник – д.т.н., проф. Захаров І.П.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки,14,
каф. Метрології та технічної експертизи, тел. (057) 702-13-31)
e-mail: anastasiia.brikman@nure.ua, тел. (099) 042-35-95

The purpose of the report is to develop a procedure for uncertainty evaluation when mercury thermometer is calibrated. The measurand is the bias of the thermometer being calibrated, which is determined using a reference thermometer. The correlation between thermometers readings was taken into account when measurement uncertainty is estimated. An uncertainty budget has been developed.

Keywords: thermometer, calibration, measurement uncertainty, uncertainty budget.

Температурою називають фізичну величину, що характеризує ступінь нагрітости тіла. Практично всі технологічні процеси і різні властивості речовини залежать від температури. На відміну від таких фізичних величин, як довжина, маса та ін. температура є не екстенсивною (параметричною), а інтенсивною (активною) величиною. Вимірювати температуру можна тільки непрямим шляхом, ґрунтуючись на залежності від температури таких фізичних властивостей тіл, які піддаються безпосередньому вимірюванню. Для цього застосовуються спеціальні засоби вимірювальної техніки (ЗВТ) – термометри, побудовані на різних фізичних принципах.

Термометри, як ЗВТ, потребують періодичного калібрування. Калібрування – сукупність операцій, за допомогою яких за заданих умов на першому етапі встановлюється співвідношення між значеннями величини, що забезпечуються еталонами з притаманними їм невизначеностями вимірювань, та відповідними показами з пов’язаними з ними невизначеностями вимірювань, а на другому етапі ця інформація використовується для встановлення співвідношення для отримання результату вимірювання з показу.

Основним методом калібрування термометрів є їх звірення з еталонним термометром за допомогою засобу порівняння. В процесі калібрування термометра оцінюють різницю Δ між результатом вимірювання термометра, що калібрується та показом еталонного термометра, визначаючи систематичну похибку термометра, що калібрується, в точці калібрування.

Невизначеність вимірювань – це параметр, що характеризує розсіювання значень величини, яку можна обґрунтовано приписати величині, що вимірюються. Параметром може бути стандартне відхилення (або кратне йому число) або половина ширини інтервалу із установленою ймовірністю

охвату. Усі складові невизначеності в результаті вимірювання можна згрупувати в дві категорії відповідно до способу їх оцінювання:
А – складові, які оцінюються шляхом застосування статистичних методів (обробкою результатів багаторазових вимірювань).
В – складові, які оцінюються в інший спосіб (за характеристиками, з попередніх експериментів, з паспорта на прилад, методики виконання вимірювань, з довідників і т.д.).

Невизначеність вимірювань включає складові, обумовлені систематичними ефектами, в тому числі складові, пов'язані з поправками і приписаними значеннями еталонів, а також дефінітну невизначеність. Іноді поправки на оцінені систематичні ефекти не вводять, а замість цього останні розглядають як складові невизначеності вимірювань.
Базовий алгоритм оцінювання невизначеності вимірювань при виконанні метрологічних робіт включає в себе наступні операції:
1) складання модельного рівняння;
2) оцінювання вхідних величин, внесення поправок на відомі систематичні ефекти в результатах вимірювань;
3) обчислення оцінки результату вимірювань;
4) визначення стандартних невизначеностей вхідних величин;
5) визначення коефіцієнтів чутливості;
6) обчислення вкладу невизначеності кожної вхідної величини у невизначеність вимірюваної величини;
7) визначення попарних кореляцій вхідних величин;
8) обчислення сумарної стандартної невизначеності вимірюваної величини;
9) обчислення коефіцієнту охвату;
10) обчислення розширеної невизначеності вимірюваної величини;
11) запис повного результату вимірювання;
12) складання бюджету невизначеності.

В силу особливості зазначеного методу калібрування і застосовуваного при цьому засобу порівняння (термостата), при оцінюванні невизначеності вимірювань необхідно враховувати кореляцію між показами термометра, що калібрується та еталонного термометра. Тому для кожної точки калібрування шкали термометра, використовуючи метод редукції, розраховують середнє арифметичне значення різниці результатів спостережень температури термометра, що калібрується та еталонного термометрів.

У роботі була досліджена методика калібрування ртутного термометра і розроблена процедура оцінювання невизначеності вимірювань під час його калібрування. Складено бюджет невизначеності, який можна використовувати для розробки програмного засобу для автоматизації оцінювання невизначеності. Розглянутий реальний приклад оцінювання невизначеності під час калібрування ртутного термометра.

SIMULATION OF NONLINEAR DYNAMICAL SYSTEMS BASED ON VOLTERRA POLYNOMIALS IN THE FREQUENCY DOMAIN

Lomovoy V.I.
Scientificadviser - D.Sc, ProfessorPavlenko V.D.
NationalUniversity"OdessaMaritimeAcademy"
(Didrihsonast., 8, Dept. MaritimeRadioCommunication, Odessa, 65029.
Tel. +38(048) 705-85-79)
e-mail:lomovoy_vi@ukr.net

A method is proposed for constructing the Volterra approximation model of the nonlinear dynamical systems in the frequency domain using of the test polyharmonic signals of various amplitudes. The computational identification method is based on the use of the regularized least squares method and the choice of the optimal step size on amplitude of test signals. The accuracy and computational stability of identification method in the form of multidimensional frequency characteristics of amplitude and phase are in vestigated. The method improves an accuracy and stability of the identification procedure.

Is developing a method of constructing approximationVolterra model of the nonlineardynamicalsystems(NDS) [1]. Method identification is based on the approximation $y(t)$ at an arbitrary deterministic signal $x(t)$ in the form of integral power of the polynomial Volterra$N$-th order (N– order approximation model)

$$\tilde{y}_N(t) = \sum_{n=1}^{N} \hat{y}_n(t) = \sum_{n=1}^{N} \int_0^{\infty} \underset{n \text{ times}}{\ldots} \int_0^{\infty} w_n(\tau_1,\ldots,\tau_n) \prod_{i=1}^{n} x(t-\tau_i) d\tau_i . \quad (1)$$

Affirmation 1. Let the input test signals NDS are fed alternately $a_1x(t)$, $a_2x(t)$, ,…,$a_Lx(t)$; a_1, a_2,…,a_L– distinct real numbers satisfying the condition $|a_j| \le 1$ for $\forall j=1,2,\ldots,L$; then

$$\tilde{y}_N[a_j x(t)] = \sum_{n=1}^{N} \hat{y}_n[a_j x(t)] = \sum_{n=1}^{N} a_j^n \int_0^{\infty} \underset{n \text{ times}}{\ldots} \int_0^{\infty} w_n(\tau_1,\ldots,\tau_n) \prod_{i=1}^{n} x(t-\tau_i) d\tau_i = \sum_{n=1}^{N} a_j^n \hat{y}_n(t) . \quad (2)$$

The partial components in the approximation model $\hat{y}_n(t)$ arefound using the least square method. This makes it possible to obtain such evaluation in which the sum of squared deviations of responses identified the nonlinear dynamical system $y[a_j x(t)]$ on the model $\hat{y}_N[a_j x(t)]$ response is minimal, i.e., NDS provides a minimum criterion

$$J_N = \sum_{j=1}^{L} \left(y[a_j x(t)] - \tilde{y}_N[a_j x(t)] \right)^2 = \sum_{j=1}^{L} \left(y_j(t) - \sum_{n=1}^{N} a_j^n \hat{y}_n(t) \right)^2 \to \min , \quad (3)$$

where $y_j(t) = y[a_j x(t)]$. Minimization of the criterion (3) is reduced to solving the system of normal equations of Gauss, which in vector-matrix form can be written as

$$\mathrm{A}'\mathrm{A}\hat{\mathrm{y}} = \mathrm{A}'\,\overline{\mathrm{y}}, \quad (4)$$

where

$$\mathrm{A}=\begin{bmatrix} a_1 & a_1^2 & \cdots & a_1^N \\ a_2 & a_2^2 & \cdots & a_2^N \\ \cdots & \cdots & \cdots & \cdots \\ a_L & a_L^2 & \cdots & a_L^N \end{bmatrix},\ \overline{\mathrm{y}}=\begin{bmatrix} y_1(t) \\ y_2(t) \\ \cdots \\ y_L(t) \end{bmatrix},\quad \hat{\mathrm{y}}=\begin{bmatrix} \hat{y}_1(t) \\ \hat{y}_2(t) \\ \cdots \\ \hat{y}_N(t) \end{bmatrix}.$$

From (4) we obtain

$$\hat{\mathrm{y}}=(\mathrm{A}'\mathrm{A})^{-1}\mathrm{A}'\overline{\mathrm{y}} \tag{5}$$

For identification in the frequency domain the test polyharmonic signals are used. We prove:

Affirmation 2. If test polyharmonic signal is used in form

$$x(t)=A\sum_{k=1}^{n}\cos\omega_k t=\frac{A}{2}\sum_{k=1}^{n}\left(e^{j\omega_k t}+e^{-j\omega_k t}\right), \tag{6}$$

then the *n*-th partial component of the response of test system can be written in the form:

$$y_n(t)=\frac{A^n}{2^{n-1}}\sum_{m=0}^{\mathrm{E}(n/2)}C_n^m\sum_{k_1=1}^{n}\ldots\sum_{k_n=1}^{n}\left|W_n\left(-j\omega_{k_1},\ldots,-j\omega_{k_m},j\omega_{k_{m+1}},\ldots,j\omega_{k_n}\right)\right|\times$$

$$\times\cos\left(\left(-\sum_{l=0}^{m}\omega_{k_l}+\sum_{l=m+1}^{n}\omega_{k_l}\right)t+\arg W_n\left(-j\omega_{k_1},\ldots,-j\omega_{k_m},j\omega_{k_{m+1}},\ldots,j\omega_{k_n}\right)\right), \tag{7}$$

whereE()– function used to obtain the of integer part of the value.The component with frequency$\omega_1+\ldots+\omega_n$is extracted from the response to test signal (7):

$$A^n\,|W_n(j\omega_1,\ldots,j\omega_n)|\cos[(\omega_1+\ldots+\omega_n)t+\arg W_n(j\omega_1,\ldots,j\omega_n)]. \tag{8}$$

Certain limitations should be imposed while choosing of frequencespolyharmonic test signals in the process determine multidimensional AFC and PFC[2].To improve the accuracy and computational stability of the identification procedure, the regularization method is applied A.N. Tikhonov and noise reduction to the obtained estimates of AFC and PFCbased on the wavelet-transform.The application package programs for dynamical systems identification in frequency domain is designed using Matlab language.

References

1. Павленко В.Д.,and ЛомовойВ.І. (2018), “Побудова апроксимаційної моделі нелінійної динамічної системи у вигляді полінома Вольтерра”.*Вчені записки Таврійського національного університету імені В.І. Вернадського*. Серія: Технічні науки. Том 29 (68), № 6. С. 200-205.

2. Pavlenko V.,SperanskyyV., IlyinV., andLomovoyV.(2012), “Modified Approximation Method for Identification of Nonlinear Systems Using Volterra Models in Frequency Domain”.*Applied Mathematics in Electrical and Computer Engineering*: Proc. of the AMERICAN-MATH'12 & CSST'12 & CEA'12, Harvard, Cambridge, USA, January 25-27. Published by WSEAS Press.P.423-428.

ЯКІСТЬ, СТАНДАРТИЗАЦІЯ ТА ВЗАЄМОЗАМІННІСТЬ МАШИНОБУДІВНОЇ ПРОДУКЦІЇ

Мартинов М. А.
Науковий керівник – к.т.н., доц. Дегтярьов О.В.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. МТЕ, тел. (057) 702-13-31),
E-mail: d_mme@nure.ua

This work is aimed at improving the standardization system for transitional fits of smooth cylindrical joints, as well as at improving metrological support of measurements and control of linear parameters of smooth cylindrical joints. The object of study - the accuracy characteristics of the mates of parts - smooth cylindrical joints with transitional fit. To achieve this goal, a probabilistic-statistical method for calculating the parameters of transitional landings is proposed, which ensures interchangeability and quality of parts. A technique is proposed for selecting universal measuring instruments for monitoring the parameters of smooth cylindrical joints.

У центр економічної політики на сучасному етапі поставлено завдання всебічного підвищення технічного рівня і якості продукції, яка повинна втілювати новітні технології, задовольняти високі техніко-економічні, естетичні та інші вимоги споживачів. Якість – ступінь відповідності сукупності властивих характеристик об'єкта вимогам [1].

Підвищення якості вітчизняної продукції в умовах ринкової економіки є однією зі складових механізму прискорення соціально-економічного розвитку суспільства, вимагає посилення дієвості державних стандартів на її технічний рівень. Стандартизація є однією з областей, яка синтезує в собі наукові, технічні, господарські та економічні аспекти. Розвиток економіки, підвищення рівня виробництва, поліпшення якості продукції, зростання життєвого рівня тісно пов'язані з широким використанням принципів стандартизації.

Стандартизація займає важливе місце в забезпеченні якості продукції машинобудівної галузі. Вироби машинобудівної галузі складаються з деталей, які з'єднані певним чином. Третю частину всіх видів з'єднань деталей в машинобудуванні складають гладкі циліндричні з'єднання. Тому проведення робіт по стандартизації в цій галузі є актуальним завданням.

В рамках даної теми досліджень проводились роботи по стандартизації перехідних посадок гладких циліндричних з'єднань, а також удосконалення метрологічного забезпечення вимірювань і контролю лінійних параметрів гладких циліндричних з'єднань.

Виконувалися розрахунки перехідною посадки типу *H/n*. Посадка *H/n* – посадка кращого використання. Дані посадки використовуються для центрування деталей в нерухомих з'єднаннях, які передають великі зусилля, при наявності вібрацій і ударів (з додатковим кріпленням). При

невеликих навантаженнях, наприклад, в приладобудуванні, вони забезпечують нерухомість з'єднання без додаткового кріплення.

Визначили максимальний і мінімальний натяг посадки $\varnothing 65H7/n6$:

$$N_{\max} = es - EI = 39 - 0 = 39\,мкм;$$

$$N_{\min} = ei - ES = 20 - 30 = -10\,мкм;$$

$$S_{\max} = -N_{\min} = 10\,мкм.$$

Средній натяг: $N_m = \left(N_{\max} + N_{\min}\right)/2 = (39-10)/2 = 14{,}5\,мкм$.

Допуски:

отвору $T_D = ES - EI = 30 - 0 = 30\ мкм$;

валу $T_d = es - ei = 39 - 20 = 19\,мкм$.

Визначили середнє квадратичне відхилення посадки за формулою:

$$\sigma_{П} = \frac{\sqrt{T_D^2 + T_d^2}}{6} = \frac{\sqrt{30^2 + 19^2}}{6} = 5{,}9\ мкм.$$

Визначили границі інтегрування:

$$z = \frac{N_m}{\sigma_{П}} = \frac{14{,}5\,мкм}{5{,}9\,мкм} = 2{,}46.$$

Побудована функція розподілу ймовірності зазорів – натягів для даної посадки.

Визначено ймовірність отримання натягів в межах від 0 до $N_m = 14{,}5\ мкм$: $\Phi(2) = \Phi(2{,}46) = 0{,}493$.

Ймовірність натягів при $z > 0$: $P_N^{'} = 0{,}5 + \Phi(z) = 0{,}993$,

або $P_N = P_N^{'} \cdot 100\% = 0{,}993 \cdot 100\% = 99{,}3\%$.

Ймовірність зазорів:

$P_S^{'} = 1 - 0{,}993 = 0{,}007$, або $P_S = P_S^{'} \cdot 100\% = 0.007 \cdot 100\% = 0{,}7\ \%$.

Значення P_N и P_S показують, що даний метод розрахунку забезпечує рекомендації стандарту ISO 286:2010 [2,3] до перехідних посадок:

$$P_{N\,табл} = (99{,}1 - 99{,}6)\ \%;$$

$$P_{S\,табл} = (0{,}9 - 0{,}4)\ \%.$$

Список використаних джерел:

1. ДСТУ ISO 9000:2015 Системи управління якістю. Основні положення та словник термінів (ISO 9000:2015, IDT) [Текст]. – Введ. 2017-01-01. – Київ: УкрНДНЦ, 2016, 50 с.

2. ISO 286-1 : 2010 ISO system of limits and fits – Part 1: Bases of tolerances, deviation and fits.

3. ISO 286-1 : 2010 Geometrical product specifications (GPS) – ISO code system for tolerances on linear sizes – Tables of standard tolerance classes and limit deviations for holes and shafts.

ОПТИМІЗАЦІЯ ЗА ДОПОМОГОЮ ВЕЙВЛЕТ-ФИЛЬТРАЦІЇ

Мироненко Е.О.
Науковий керівник – к.т.н., проф. Білоус Н.В.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки,14, каф. Програмної інженерії,
тел. (057) 702-14-46)
e-mail: eduard.myronenko@nure.ua, факс (057) 746-72-99

The paper considers the optimization of waveletfiltration algorithms with two-parameter threshold functions. Optimization of wavelet-filtering algorithms is performed in two directions: a) optimization by choosing the best threshold function from the functions used in practice; b) optimization by estimating the optimal parameters of the best threshold function.

В роботі розглядається оптимізація алгоритмів вейвлетфільтрациі з двопараметричного пороговими функціями. Оптимізація алгоритмів вейвлет-фільтрації виконується в двох напрямках: а) оптимізація за рахунок вибору найкращої порогової функції з використовуваних на практиці функцій; б) оптимізація шляхом оцінювання оптимальних параметрів найкращою порогової функції.

Теоретичною основою порогових алгоритмів вейвлет-фільтрації є наступна передумова: рівень коефіцієнтів розкладання випадкових помилок вихідних порівняно малий у порівнянні з коефіцієнтам розкладання точного сигналу, що дозволяє розпізнати дві ситуації: «Шумовий» коефіцієнт (в основному обумовлений шумом вимірювання) і «Інформативний» коефіцієнт (в основному визначається значеннями точного сигналу).

Таким чином, для успішної фільтрації необхідно звернути в нуль шумові коефіцієнти, зберігши при цьому інформативні коефіцієнти розкладання. Ця ідея реалізується граничними алгоритмами обробки «зашумлених» коефіцієнтіврозкладання.

На практиці широко використовуються дві порогові функції:

- «жесткая» пороговая функция виду(1)

$$T_h(\tilde{d},\lambda)=\begin{cases}0, \text{якщо } |\tilde{d}|\le\lambda\\ \tilde{d}, \text{якщо } |\tilde{d}|>\lambda\end{cases} \quad (1)$$

- «мягкая» пороговая функция

$$T_s(\tilde{d},\lambda)=\begin{cases}0, \text{якщо } |\tilde{d}|\le\lambda\\ sign(d)*\left[|\tilde{d}|-\lambda\right], \text{якщо } |\tilde{d}|>\lambda\end{cases} \quad (2)$$

, де λ - величина порога, $\tilde{d}$ – оброблюваний коефіцієнт розкладання (як правило – це деталізують коефіцієнти, відносно похибка яких на порядок і більше вище, ніж у аппроксимирующих коефіцієнтів (див. [2], стор. 58-60).

Графіки функцій (1), (2) наведені на рисунку 1 для λ = 1 (1 - графік функції (1), 2 - функція (2)). Відзначимо характерні особливості цих функцій:

- через зменшення амплітуди коефіцієнта розкладання на величину λ в функції T d S (, λ) можливо згладжування (розмиття) контрастних елементів оброблюваного сигналу, особливо при великих значеннях λ;
- наявність у функції T d H (, λ) розриву в околиці λ може викликати появу осциляцій (ефект Гіббса) в «особливих» точках оброблюваного сигналу.

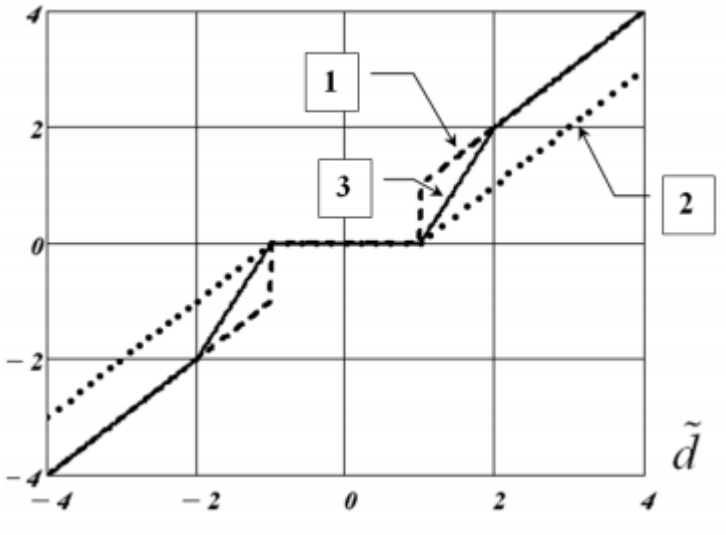


Рисунок 1. Графіки граничних функцій (1), (2)

Очевидно, що різну поведінку цих функцій обумовлює різну помилку алгоритмів вейвлет-фільтрації з використанням двопараметричних порогових функцій. виникає нетривіальний питання: яка з трьох наведених вище порогових функцій має меншу помилку фільтрації? Відповідь на це питання дав змогу б рекомендувати цю функцію для використання на практиці і перейти до оцінки оптимальних параметрів цієї функції.

Перелік посилань:

1)Mallat S. A theory of multiresolution signal decomposition: the wavelet representation. IEEE Trans. Pattern Anal. Machine Intell. 1989. v.11. N 9. P. 674-693.

2)Воскобойников Ю.Е. Вейвлет-фильтрации сигналов и изображений (с примерами в Mathcad) Новосибирск: НГАСУ (Сибстрин), 2015. 196 с.

РОЗРОБКА МЕТРОЛОГІЧНОГО ЗАБЕЗПЕЧЕННЯ КАЛІБРУВАНЬ ЗАСОБІВ ВИМІРЮВАННЯ ГЕОМЕТРИЧНИХ РОЗМІРІВ

Пахомова А.О., Фоменко В.Д.
Науковий керівник – к.т.н., доц. Дегтярьов О.В.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. МТЕ, тел. (057) 702-13-31),
E-mail: d_mme@nure.ua

The system of accounting and documenting the results of the verification of the suitability of measuring instruments for operation is proposed. A local validation scheme has been developed. The method of carrying out calibration of measuring instruments of geometric quantities, which provide the correct and unified procedure of calibration, is developed. Methods of comparative analysis of existing verification methods, national and international normative base in the field of metrological support of measuring instruments of geometric quantities, methods of statistical processing of measurement results are used.

Вимірювання – це невід'ємна частина технологічних процесів, які безпосередньо впливають на якість продукції. Вимірювальна інформація служить основою для прийняття рішень про якість продукції, при впровадженні систем якості, і тільки достовірність і відповідна точність результатів вимірювань забезпечує правильність прийнятих рішень на всіх рівнях управління. Якість – ступінь відповідності сукупності властивих характеристик об'єкта вимогам [1]. Якість вимірювань залежить від якості метрологічного забезпечення.

Під метрологічним забезпеченням (МЗ) розуміється встановлення і застосування наукових і організаційних основ, технічних засобів, правил і норм для забезпечення єдності і необхідної точності вимірювань. МЗ є комплексним поняттям, і включає такі складові, як розробка та атестація засобів вимірювальної техніки, метрологічна експертиза технічної документації, повірка та калібрування засобів вимірювальної техніки, розробка та атестація методик виконання вимірювань, атестація випробувального обладнання. МЗ виробництва включає технічні засоби, правила і норми, що забезпечують повноту, точність і достовірність контролю якості продукції на всіх етапах. Досягнення високої якості продукції та ефективності виробництва, забезпечення необхідної точності, взаємозамінності і достовірного обліку продукції, що випускається – основні цілі МЗ виробництва. У промисловості вимірювання геометричних величин (довжин; діаметрів; кутів; відхилень форми і розташування поверхонь; шорсткості поверхонь; зазорів) є основою перевірки контролю якості, обліку кількості продукції і управління сучасними технологічними процесами.

Важливим елементом забезпечення якості вимірювань є відповідність засобів вимірювань і процесів вимірювань вимогам

стандартів ISO, зокрема, ДСТУ ISO 10012 [2]. Цей стандарт передбачає проведення калібрувань. Калібрування – визначення в заданих умовах або контроль метрологічних характеристик ЗВТ. Основні положення з калібрування ЗВТ регламентує ДСТУ 3989 [3].

Для досягнення цілей підприємства з управління якістю в роботі запропоновані система обліку і документування результатів перевірки придатності засобів вимірювань до експлуатації, розроблена локальна повірочна схема, розроблені методики проведення калібрування засобів вимірювань геометричних величин , що забезпечують правильний і єдиний порядок проведення калібрування (табл.1).

Таблиця 1 – Процедури калібрування

Найменування операції	Засоби калібрування і їх нормативно-технічні характеристики
Визначення довжини вильоту губок штангенциркулів	Лінійка вимірювальна металева за ДСТУ ГОСТ 427: 2009 Лінійки через вимірювальні металеві. Технічні умови
Визначення відхилення від площинності і прямолінійності вимірюваних поверхонь губок	Лінійка лекальна типу ЛД кл. т. 1 за ГОСТ 8026-92 Лінійки повірочні. Технічні умови"
Визначення відхилення від паралельності плоских вимірювальних поверхонь губок	Пласкопаралельні кінцеві міри довжини кл. т. 2, 4-й розряд за ДСТУ ГОСТ 9038: 2009 Міри довжини кінцеві плоскопаралельні. Технічні умови
Визначення розміру зсунутих до зіткнення губок і відхилення від паралельності утворюють вимірювальних поверхонь губок для внутрішніх вимірювань	Мікрометр типу МК, межа вимірювання 0-25 мм, кл. т. 2 за ДСТУ ГОСТ 6507: 2009 Мікрометри. Технічні умови
Визначення похибки штангенциркулів	Пласкопаралельні кінцеві міри довжини кл. т. 2, 4-й розряд за ДСТУ ГОСТ 9038: 2009. Нутромер мікрометричний за ДСТУ ГОСТ 10: 2009 Нутромери мікрометричні. Технічні умови

В результаті вдосконалення процедур з управління якістю вимірювальним оснащенням кількість претензій споживачів щодо якості продукції підприємства за перше півріччя 2018 знизилась на 40 %.

Список літератури:

1. ДСТУ ISO 9000:2015 Системи управління якістю. Основні положення та словник термінів (ISO 9000:2015, IDT) [Текст]. – Введ. 2017-01-01. – Київ: УкрНДНЦ, 2016, 50 с.

2. ДСТУ ISO 10012:2005 Системи управління вимірюваннями. Вимоги до процесів вимірювання та вимірювального оснащення.

3. ДСТУ 3989-2000 Метрологія. Калібрування засобів вимірювальної техніки. Основні положення, організація, порядок проведення та оформлення результатів.

ОСОБЕННОСТИ ПЕРЕОПРЕДЕЛЕНИЯ КИЛОГРАММА - ОСНОВНОЙ ЕДИНИЦЫ SI

Паценко А. Н.
Научный руководитель – д.т.н., проф. Захаров И. П.
Национальный научный центр «Институт метрологии»
(61002, Харьков, ул. Мироносицкая, 42, тел. (057) 700-34-09)
e-mail: sashapatsenko@ukr.net

From May 20, 2019, the SI will be based on seven physical constants, and thus inherently stable. Most notably, this will mark the end of the last remaining physical artefact in the SI system – a cylinder of metal known as the International Prototype of the Kilogram.

In the context of the future definition of the mass unit, a promising approach is to link the kilogram to the Planck constant using, for example watt-balance.

Keywords: kilogram, watt-balance, Planck constant, Avogadro constant.

Килограмм – единица измерения массы, одна из семи основных единиц Международной системы единиц (SI). До недавнего времени килограмм являлся последней единицей SI, которая была привязана к рукотворному артефакту – цилиндру диаметром и высотой 39,17 мм из платино-иридиевого сплава (90 % платины, 10 % иридия), который хранится в Международном бюро мер и весов, г. Севр, Франция).

Международный эталон килограмма практически не подвергается какому-либо перемещению или использованию. Его копии хранятся в национальных метрологических учреждениях по всему миру. В 1889, 1948, 1989 и 2014 годах проводились верификации копий с эталоном с целью обеспечить единство измерений массы относительно эталона.

Результаты показали, что массы эталонов-копий меняются относительно главного эталона в диапазоне ± 50 микрограммов за 100 лет.

Насколько при этом изменилась масса главного эталона — неизвестно, поскольку его не с чем сравнивать. Для многих типов измерений такое отклонение может привести к недостоверным результатам.

26 ноября 2018 г. участники 26-й Генеральной конференции по мерам и весам, которая проходит в Париже, приняли историческое решение о переопределении четырех из семи основных единиц SI — килограмма, ампера, кельвина и моля.

Этим решением килограмм больше не связан с материальным носителем-эталоном, и теперь определяется через постоянную Планка, которая в точности равна $h = 6.626\,070\,15 \times 10^{-34}$ кг · м$^{-2}$ · с$^{-1}$.

Установки, с помощью которой можно реализовать новый эталон массы, называются ватт весы, или же весы Киббла. Они позволяют измерить вес через константу Планка. Масса при этом подходе

пропорциональна произведению тока и напряжения. Электромагнитные силы в нем возникают благодаря катушке, зажатой между двумя постоянными магнитами.

Прибор имеет два режима работы. В первом электрический ток проходит через катушку и создает магнитное поле, которое взаимодействует с постоянным магнитным полем. В результате создается давление, которое позволяет сбалансировать массу килограмма.

Во втором режиме катушка поднимается с постоянной скоростью — восходящее движение индуцирует в ней напряжение, пропорциональное силе магнитного поля. Измеряя ток, напряжение и скорость катушки, исследователи могут вычислить константу Планка, которая пропорциональна количеству электромагнитной энергии, необходимой для определения баланса массы.

Второй подход разработали в Национальном метрологическом институте Германии. Там создали практически идеально гладкие сферы из кремния диаметром около 93,5 миллиметра с шероховатостью, не превышающей трех десятых нанометра, и отклонениями от сферической формы до нескольких десятков нанометров. Это настолько мало, что если такую сферу масштабировать до размеров Земли, отклонения от идеально ровной формы не будут превышать нескольких метров. Сферы сделаны из монокристалла кремния, причем одного изотопа — ^{28}Si. Кремний был выбран из-за того, что благодаря развитой полупроводниковой промышленности существуют методы получения кремниевых объектов практически идеального строения. Примесей в такой сфере настолько мало, что его масса отличается от идеальной меньше, чем на одну десятимиллионную долю грамма.

Поскольку сферу можно считать практически идеальной с точки зрения кристаллического строения и состава, а ее масса равна массе эталона килограмма, то, точно измерив ее размер, период кристаллической решетки и плотность упаковки атомов, ученые могут узнать количество атомов в ней. Исходя из этого можно получить число Авогадро, а затем постоянную Планка. На данный момент ученые смогли измерить число Авогадро с неопределенностью в 20 миллиардных долей.

Для создания эталона массы будет применяться баланс Киббла, вычисление константы Планка происходит с беспрецедентной точностью.

Реформа вступит в силу 20 мая 2019 г. С этого момента все единицы системы SI привязаны к фундаментальным физическим константам.

Литература:

1. 2018 Press Kit of the 26th CGPM www.bipm.org/utils/en/pdf/CGPM-Press-Kit.pdf

2. 2018 Resolution 1 of the 26th CGPM www.bipm.org/en/CGPM/db/26/1/

3. 2014 Resolution 1 of the 25th CGPM www.bipm.org/en/CGPM/db/25/1/

ДИНАМІЧНІХАРАКТЕРИСТИКИВИМІРЮВАЛЬНИХ ПЕРЕТВОРЮВАЧІВНАБАЗІШТУЧНИХНЕЙРОННИХМЕРЕЖПРИ ЗАСТОСУВАННІАДАПТИВНОГОАЛГОРИТМУ

Фоменко В. Д., Пахомова А. О.
Науковийкерівник – к.т.н., доц. Сергієнко М.П.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. МТЕ, тел. (057)702-13-31)
E-maill: d_mme@nure.ua

Application of adaptive identification method dynamiccharacteristics of measuring instruments by impulse characteristics based on artificial neural networks. At present, artificial neural networks (INS) that are capable of learning from existing data are used to solve many metrological problems. The purpose of this work subsection is the development and application of an adaptive method based on the INS for identifying SIT parameters modeled by dynamic links of the aperiodic and vibrational types according to impulse characteristics.

В даний час для вирішення багатьох метрологічних завдань знаходять застосування штучні нейронні мережі (ШНМ), здатні до навчання на основі наявних даних. Метою даного підрозділу роботи є розробка і застосування адаптивного методу на базі ІНС для ідентифікації параметрів ЗВТ, що моделюються динамічними ланками аперіодичного і коливального типів, по імпульсним характеристикам.

Для реалізації адаптивного методу ідентифікації параметрів ЗВТ з імпульсною характеристикою $g(t)$ застосовується багатошарова рекуррентная ІНС. Перший шар ІНС є адаптивних учнів мережу, що складається з m нейтронів, на вхід кожного з яких подається навчальне вплив.

Спочатку m значень y_k (в залежностівідмоделі y_k відповдає T_k та/або ξ_k, $k = 1 \ldots m$) задаються довільно з рівномірним інтервалом

$$y_k = y_{\min} + k\frac{y_{\max} - y_{\min}}{m} \quad .(1)$$

Навчання засноване на мінімізації середньоквадратичних помилок мережі

$$Q = \sum_{k=1}^{m} \delta_k^2 = \frac{1}{2}\sum_{k=1}^{m} (y_k - \varphi_k)^2 \quad ,(2)$$

де функція активації φ_k внаслідок нелинійності $g(y_k)$ описується логістичною функцією

$$\varphi_k = \varphi(u_{yk}) = \frac{1}{1 + \exp(-wy_k^{\mathrm{T}}\, g(y_k))} \quad ,(3)$$

де wy_k^{T} – k-та строка транспонованої матриці синаптичних ваг, що визначаються як функція мінімуму помилки мережі

$$wy_{ki} = f(Q_{\min}). \quad (4)$$

Таким чином, результатом навчання ІНС є отримання матриці синаптичних ваг wy_{ki}, відповідних мінімуму Q.

Після навчання мережі на її вхід подаються дискретні значення вимірювальної величини. Розраховується середня квадратична помилка мережі за формулою

$$Q = \frac{1}{2}\sum_{k=1}^{m}(y_k - y_{xk})^2, \quad (5)$$

і визначається значення задається параметра y_k, при якому спостерігається мінімальна помилка $\delta_{\min}$.Слід зазначити, що збільшення Q на проміжних етапах ідентифікації може свідчити про неправильне навчання мережі, тому в таких випадках слід повернутися до попередньої ітерації і збільшити інтервал заданих значень y_k.

Список літератури:

1) Альравашдех Бакер Применение адаптивного алгоритма идентификации динамических характеристик измерительных преобразователей на базе искусственных нейронных сетей / БакерАльравашдех, М.П. Сергиенко // Системы обработки информации, 2015. – № 6 (131). – С. 6 – 9.

2) Водотыка С.В. Использование искусственных нейронных сетей при построении калибровочной зависимости средства измерения / С.В. Водотыка // Системиобробкиінформації, 2011. – Вип. 1(91). – С. 24 – 27.

3) Дегтярев А.В. Адаптивная система компенсации нелинейности функции преобразования измерительных устройств на базе трехслойного персептрона / А.В. Дегтярев, О.В. Запорожец, Т.А. Овчарова // Електротехнічні та комп'ютернісистеми, 2012. – № 6. – С. 235 – 241.

4) Волосников А.С. Линейная нейросетевая динамическая измерительная система с последовательным восстановлением и фильтрацией входного сигнала датчика [Текст] / А.С. Волосников // Изв. Челяб. Науч. Центра. – 2006. – № 1(31). – С. 90 – 95.

ОЦІНКА НЕВИЗНАЧЕНОСТІ РЕЗУЛЬТАТІВ ВИМІРЮВАНЬ КОНДУКТИВНОГО ПАРАЗИТНОГО ВИПРОМІНЮВАННЯ МЕТОДОМ ПРЯМОГО ЗЧИТУВАННЯ

Штефан І.Ю.
Науковий керівник – д.т.н., проф. Захаров І.П.
Харківськийнаціональний університет радиоелектроніки
(61166, Харків, пр.Науки,14, каф. Метрології та технічної експертизи,
тел. (057) 702-13-31)
e-mail: ivan.shtefan@nure.ua

The given work is devoted to the development of a procedure of estimating of uncertainty of measurements. The model equation is recorded, the numerical values of the input values are estimated, the numerical value of the measured value is calculated, the standard uncertainties of the input quantities, the sensitivity coefficients, the total standard uncertainty, and the expanded uncertainty are estimated. The uncertainty budget is given.

Однією з вимог щодо акредитації випробувальних та калібрувальних лабораторії за ДСТУ ISO/IEC 17025:2006 [1] є необхідність мати та застосовувати процедуру оцінювання невизначеності вимірювань.

Відповідно до ДСТУ ETSIEN 300 220-2:2012 [2] методика вимірювання паразитного випромінювання методом прямого зчитування полягає в наступному. Передавач, що тестується, з'єднується з аналізатором спектру за допомогою атенюатора і фільтра, і абсолютне зчитування отримується на аналізаторі для кожного побічного випромінювання. Аналізатор спектру, атенюатор та фільтр є відкаліброваними на частоті паразитного випромінювання.Втрати в кабелі є незначними і тому не враховуються.

Модельне рівняння вимірювання має вигляд:

$$P_{\text{п}} = 10^{(A+K_{\text{а}}+K_{\text{ф}}+P_0)} \qquad (1)$$

де $P_{\text{п}}$ – потужність кондуктивного паразитного випромінювання, мВт; P_0 – показ аналізатора спектру, дБмВт; $A_{\text{а}}$ – коефіцієнт втрататенюатору, дБ; $K_{\text{ас}}$ – коефіцієнт калібрування аналізатора спектру, дБ; $K_{\text{ф}}$ – коефіцієнт калібрування фільтру, дБ.

Значення потужності $\widehat{P}_0$ оцінюється за результатами одноразових вимірювань потужності аналізатором спектру. Значення коефіцієнту ослаблення атенюатору $\widehat{A}$, коефіцієнту калібрування фільтру $\widehat{K}_{\text{ф}}$ та коефіцієнтукалібрування аналізатора спектру $\widehat{K}_{\text{ас}}$ беруться з сертифікатів їх калібрувань.

Розраховується значення вимірюваної величини.

Оцінювання сумарної стандартної невизначеності здійснюється за формулою

$$u_c(P_{\text{п}}) = 0,23P_{\text{п}}\sqrt{u^2(A) + u^2(K_{\text{ф}}) + u^2(K_{\text{ас}}) + u^2(P_0)}\,, \qquad (2)$$

де – стандартна невизначеність вимірюваннякоефіцієнту калібрування аналізатора спектру

$$u(K_{\text{ас}}) = \frac{U_{\text{ас}}}{k_{\text{ас}}}; \qquad (3)$$

тут $U_{\text{ас}}$ – розширена інструментальна невизначеність аналізатора спектру, $k_{\text{ас}}$– коефіцієнт охоплення, які беруться з сертифікату калібрування аналізатора спектру для частоти паразитного випромінювання;

$u(P_0)$ – стандартна невизначеність, яка обумовлена повторюваністю вимірювань аналізатора спектру, приймається рівною середньоквадратичному відхиленню повторюваності s_r результатів вимірювання потужності, яка визначається при попередніх вимірюваннях;

$u(A)$ – стандартна невизначеність вимірювання ослаблення атенюатору

$$u(A) = \frac{U(A)}{k_A}, \qquad (4)$$

тут $U(A)$ – розширена невизначеність вимірювання ослаблення атенюатору, k_A – коефіцієнт охоплення, які беруться з сертифікату калібрування атенюатору для частотипаразитного випромінювання;

$u(K_{\text{ф}})$ стандартна невизначеність вимірюваннякоефіцієнту калібрування фільтру

$$u(K_{\text{ф}}) = \frac{U_{\text{ф}}}{k_{\text{ф}}}; \qquad (5)$$

тут $U_{\text{ф}}$ – розширена інструментальна невизначеність фільтру, $k_{\text{ф}}$ – та коефіцієнт охоплення, які беруться з сертифікату калібрування фільтру для частотипаразитного випромінювання.

Оцінюється розширена невизначеність вимірювань та записується результат вимірювань в стандартному вигляді. Наводиться бюджет невизначеності

Списокджерел:

1. ДСТУ ISO/IEC 17025:2006. – Введ. 01.07.07. – Київ: Держспоживстандарт України, 2007. - 32 с. 2. ДСТУ ETSI EN 300 220-2:2012 Електромагнітна сумісність та радіочастотний спектр. Радіообладнання малого радіусу дії діапазону частот від 25 МГц до 1000 МГц з рівнем потужності до 500 мВт. Частина 2. Загальні технічні вимоги. – Введ. 01.05.13. – Київ: Держспоживстандарт України, 2013.

РОЗРОБКА МЕТРОЛОГІЧНОГО ЗАБЕЗПЕЧЕННЯ КОНТРОЛЮ ЯКОСТІ ПРОДУКЦІЇ МАШИНОБУДУВАННЯ

Юношев Д.Є.
Науковий керівник – к.т.н., доц. Дегтярьов О.В.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. МТЕ, тел. (057) 702-13-31),
E-mail: d_mme@nure.ua

Metrological control of smooth cylindrical joints has been improved. A comparative analysis of the existing normative base on the tolerances and landing of smooth cylindrical joints, calibre-scraps, calibre-plugs, methods of calculating the planting parameters, methods of statistical processing of measurement results is made. The proposed method of calculating calibers for controlling external elements of parts, providing interchangeability and quality of parts. The method of choice of universal means of measuring equipment for control of parameters of smooth cylindrical joints is offered.

Якість – головна мета і основна рушійна сила розвитку суспільства. Згідно ISO 9000:2015 [1] якість – ступінь відповідності сукупності присущих характеристик об'єкта вимогам.

Всі види діяльності людини підпорядковані одному: підвищення якості життя. А в сфері матеріального виробництва: поліпшення якості продукції, що виробляється [2].

Особливе місце якість займає у виробництві продукції машинобудування – головної галузі економіки будь-якої держави. Продукція, що випускається машинобудівною промисловістю це машини, верстати, прилади, інструменти і пристосування, які складаються з деталей різноманітних форм і розмірів. Для машинобудування найефективнішими показниками якості є експлуатаційні характеристики машин. Експлуатаційні показники механізмів і машин (довговічність, надійність, точність і т. д.) в значній мірі залежать від правильності вибору посадок, допусків форми і розташування, шорсткості поверхні.

При проектуванні деталей машин їх геометричні параметри задаються розмірами елементів, а також формою і взаємним розташуванням їх поверхонь. При виготовленні виникають відхилення геометричних параметрів реальних деталей від запроектованих значень. Ці відхилення називаються похибками.

Вимірювання є головним джерелом відомостей про відповідність продукції встановленим вимогам. Для контролю відповідності встановленим вимогам використовують контрольно-вимірювальні інструменти. Тому для забезпечення належної якості проектування, виготовлення деталей, вузлів і машин важливим є питання метрологічного забезпечення контролю та вимірювань параметрів якості виробів.

При масовому виробництві деталей, для спрощення визначення придатності деталей часто перевіряють, чи знаходиться дійсне значення розмірів деталей в установлених межах. Тому процес отримання та обробки інформації про об'єкт для визначення його придатності чи непридатності називають контролем.

Для того щоб визначити придатність деталі необхідно визначити її дійсні розміри. Відхилення дійсного розміру деталі від номінального для заданого квалітету не повинно виходити за межі допуску, встановленого стандартами ISO 286: 2010 [3,4].

Об'єктом контролю якості є вал з параметрами $\varnothing 60k6$. Для контролю деталей, виготовлених за даним квалітетом пропонується використовувати калібри. Калібри – безшкальні вимірювальні інструменти, призначені для контролю розмірів елементів деталей, їх геометричної форми і взаємного розташування. Основним перевагою калібрів є висока продуктивність контролю - економія часу на проведення контрольно-вимірних операцій. За допомогою калібрів можна визначити дійсні розміри елементів деталей. Завданням контрольних функцій калібрів є встановлення відповідності дійсних розмірів елементів деталей та їх граничних значень, проставленим в робочих кресленнях, на основі чого робляться висновки про придатність або непридатність деталі по її контрольованим параметром. Вал $\varnothing 60k6$ є придатний, якщо дійсний розмір більше ніж найменший граничний розмір і менше ніж найбільший граничний розмір, тобто $d_{\min} < d_{Д} < d_{\max}$. Зі схеми розміщення поля допуску вала слідує, що якщо дійсний розмір знаходиться в межах допуску, то вал придатний.

Визначено допуски і граничні відхилення калібру. Для діаметра $\varnothing 60$ мм 6-го квалітету точності виконавчі розміри калібрів: ПР = $60{,}0145^{+0{,}005}$мм; НЕ = $59{,}9995^{+0{,}005}$ мм.

Для досягнення поставленої в роботі мети запропонований метод розрахунку калібрів для контролю зовнішніх елементів деталей, що забезпечує взаємозамінність і якість деталей. Запропоновано методику вибору універсальних засобів вимірювальної техніки для контролю параметрів гладких циліндричних з'єднань.

Список використаних джерел:

1. ДСТУ ISO 9000:2015 Системи управління якістю. Основні положення та словник термінів (ISO 9000:2015, IDT) [Текст]. – Введ. 2017–01–01. – Київ: УкрНДНЦ, 2016, 50 с.

2. ДСТУ ISO 9001:2015 Системи управління якістю. Вимоги (ISO 9001:2015, IDT). – Введ. 2016-07-01. – Київ: УкрНДНЦ, 2016. – 31 с.

3. ISO 286-1 : 2010 ISO system of limits and fits – Part 1: Bases of tolerances, deviation and fits.

4. ISO 286-1 : 2010 Geometrical product specifications (GPS) – ISO code system for tolerances on linear sizes – Tables of standard tolerance classes and limit deviations for holes and shafts.

АЛФАВІТНИЙ ПЕРЕЛІК

ЗМІСТ

«РАДІОЕЛЕТРОНІКА І МОЛОДЬ У XXI СТОЛІТТІ»

МАТЕРІАЛИ 23-го МІЖНАРОДНОГО МОЛОДІЖНОГО ФОРУМУ

Відповідальний за випуск: І.В. Руженцев

Комп’ютерна верстка О.І. Ільїна, В.Г. Чепела

Підп. до друку 02.04.19. Формат 60х84 1/16. Спосіб друку – ризографія.
Умов.друк.арк. 7,3. Облік. вид.арк. 6,5. Тираж 69 прим.
Ціна договірна Зам № 2-314.

ХНУРЕ. Україна. 61166, Харків, просп. Науки, 14

Віддруковано в редакційно-видавничому відділі ХНУРЕ
61166, Харків, просп. Науки, 14