СИСТЕМИ ТЕЛЕКОМУНІКАЦІЙ

УДК 681.32.03

М.М. Климаш, Р.В. Павлюк, В.В. Павлюк
Національний університет "Львівська політехніка",
кафедра телекомунікацій

ПОБУДОВА МАТЕМАТИЧНИХ ТА ІМІТАЦІЙНИХ МОДЕЛЕЙ ДЛЯ ВИЗНАЧЕННЯ СТРУКТУРНОЇ НАДІЙНОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ

Розглянуто проблеми розробки математичних та імітаційних моделей для аналізу надійності інформаційних систем, наведено загальну архітектуру імітаційної моделі та приклад її застосування.

The scope of the paper includes a review of base problems related to the creation of mathematical and imitating models for the analysis of informational systems reliability; a general architecture of imitating model has been presented and its usage as well.

Вступ

Високий темп розвитку інформаційних технологій та їх постійно зростаюча роль в нашому повсякденному житті ставить дедалі більші вимоги щодо їх надійності та стабільності. Особливо це стосується магістральних телекомунікаційних систем, які становлять кістяк глобальної цифрової системи зв'язку. Не менш важливим є питання надійності інтегрованих обчислювальних систем, які з розвитком високошвидкісних магістральних з'єднань, все більше й більше використовуються для вирішення складних та ресурсомістких задач. Зокрема мова йтиме про так звані *розподілені інформаційні системи*.

Структурна надійність мережі

Якщо говорити про поняття *надійності* мережі, то для нього існує чимало визначень. *Надійність* елемента мережі визначається як ймовірність того, що елемент (вузол чи з'єднання) буде повністю доступним і працездатним у визначений період часу. Поняття *доступності* випливає із визначення надійності: доступність – це ймовірність того, що елемент мережі буде працездатним у певний чітко визначений момент часу. Простий приклад показано на рис. 1: для кожного з'єднання та вузла в мережі вказана його доступність. Якщо припустити, що ці ймовірності є взаємно незалежними, то ми можемо нескладно вирахувати загальну доступність всього шляху проходження цифрового потоку, враховуючи дані про доступність усіх елементів, що знаходяться на ньому. Наприклад, доступність шляху, який вказаний на цьому рисунку, становитиме:

$$0.99996 \cdot 0.9997 \cdot 0.99999 \cdot 0.9998 \cdot 0.99997 \cdot 0.9999 \cdot 0.99995 \cdot 0.9995 \cdot 0.99990 \approx 0.9987$$

Оскільки вищезгадані визначення переважно сконцентровані на статистичному поданні елементів мережі, чимало визначень описують можливості мережі загалом. *Цілісність* мережі – це здатність мережі надавати необхідну якість сервісу (Quality of Service) не лише в нормальному режимі роботи, тобто, коли відсутні збої та аварії на її складових, а також в режимі перевантажень і в аварійному режимі, коли вийшли з ладу певні її складові.

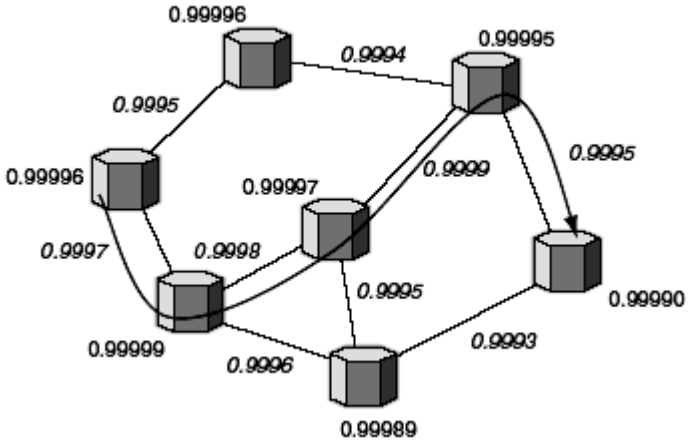


Рис. 1. Мережа із визначеними доступностями вузлів та з'єднань

Поняття цілісності також включає в себе поняття *живучості* – це здатність мережі відновити інформаційний потік в момент збою із мінімально можливими втратами для кінцевого користувача або з їх повною відсутністю, що для видів трафіку є дуже критичним. Оскільки абсолютна живучість мережі є неможливою (наприклад, у разі потужних землетрусів, що зумовлюють тотальні руйнування комунікаційних споруд), ми використовуємо певні рівні для того, щоб розрізняти межі, в яких мережа може самовідновитися у випадку поодинокого або ж багатократного збою, зважаючи на ймовірність виникнення того чи іншого збою.

Імітаційна модель захисту SDH-мережі як інформаційної системи

Щодо транспортних інформаційних мереж, то переважна їх більшість побудована за технологією SDH/SONET. Технологія SDH/SONET є технологією, що дає змогу проводити досить швидке резервне перемикання (порядку 50–60 мілісекунд). Такий показник досягається кількома чинниками: по-перше, ця технологія використовує удосконалені моніторингові процеси для виявлення, сповіщення та запобігання збоям та аваріям; по-друге, за швидкісне перемикання з ушкодженої (аварійної) ділянки на резервну відповідає *протокол автоматичного перемикання APS* (Automatic Protection Switching). Незважаючи на те, що як стратегію втілення швидкісного перемикання було взято ідею так званих захисних (резервних) кілець, тим не менше існує тенденція щодо переходу від кільцевих до коміркових топологічних структур.

Системи захисту та резервування мереж SDH поділяють на дві групи відповідно до того, як поділяються топологічні елементи. Перша група – системи захисту для кільцевих топологій (MS-SPRing, MS-DPRing, SNCP), друга – захист сегментів типу "точка-точка" (MSP, SNCP).

Нами було проведено дослідження, метою якого є знаходження механізму, а відповідно і математичної чи імітаційної моделі, яка давала б змогу отримати повну картину процесів резервування та відновлення, які відбуваються в мережі. До того ж механізм повинен мати високу адаптованість щодо його реалізації за допомогою електронних обчислювальних засобів.

Основним критерієм, якого слід було б дотримуватися під час побудови математичної моделі для проведення аналізу структурної надійності інформаційної системи, є повна її дискретність. У цьому випадку під терміном *дискретність* ми розуміємо дискретні набори параметрів елементів мережі, такі як, наприклад, множина доступностей всіх з'єднань мережі, напрямленість потоків в кожній з ланок тощо. Враховуючи це, постала потреба використати для дослідження матричні методи, оскільки саме вони дають найпрозоріше дискретне подання параметрів системи, а також є найзручнішим способом подання даних під час їх обробки за допомогою електронних обчислювальних засобів. Ця модель отримала назву *мультишарового матричного представлення* (multilayer matrix representation), оскільки в структурному плані ця модель являє собою віртуальне накладання багатьох матриць однакової розмірності одна на одну, де комірка кожного шару є значенням певного параметра елемента мережі, а сама розмірність визначається кількістю вузлів.

Модель дослідження, яка ґрунтується на мультишаровому матричному поданні, являє собою комплексний математично-логічний механізм, складається з двох основних груп компонентів (рис. 2):

- матриць даних (власне мультишарове матричне подання);
- алгоритми обробки даних.

Матриці даних призначені для подання та зберігання інформації про аналітичні та статистичні параметри елементів мережі – з'єднань та вузлів, а також мережевих топологічних утворень: кілець, комірок тощо.

Алгоритми проводять обробку даних, що містяться у матрицях, згідно з заданими математичними та логічними правилами. Алгоритми поділяються на дві групи: *алгоритми моніторингу* та *алгоритми обробки*. Завдання перших – проводити постійний моніторинг стану матриць параметрів на виявлення нестандартних ситуацій, задача алгоритмів обробки – обробка повідомлень від алгоритмів моніторингу та реалізація протоколів захисту структури мережі від втрати повнодоступності.

Сукупність матриць даних утворює тривимірний масив, що має такі властивості:

- у горизонтальних площинах знаходяться так звані *матриці параметрів*, що містять однотипні параметри міжвузлових з'єднань;
- вертикальний стовпець-переріз дає нам набір усіх визначених параметрів різних типів для конкретного міжвузлового з'єднання;
- вертикальні перерізи дають нам змогу отримати двовимірні масиви параметрів міжвузлових з'єднань, які виходять з вузла або ж входять у нього (від напрямку перерізу).

Графічно зображена ця модель на рис. 1.

Для прикладу застосування отриманої математичної моделі розглянемо конкретну задачу. Нехай маємо мережу, що складається з чотирьох вузлів *a, b, c, d*, з'єднаних так, як показано на рис. 3 (тобто двонапрямлене SDH-кільце).

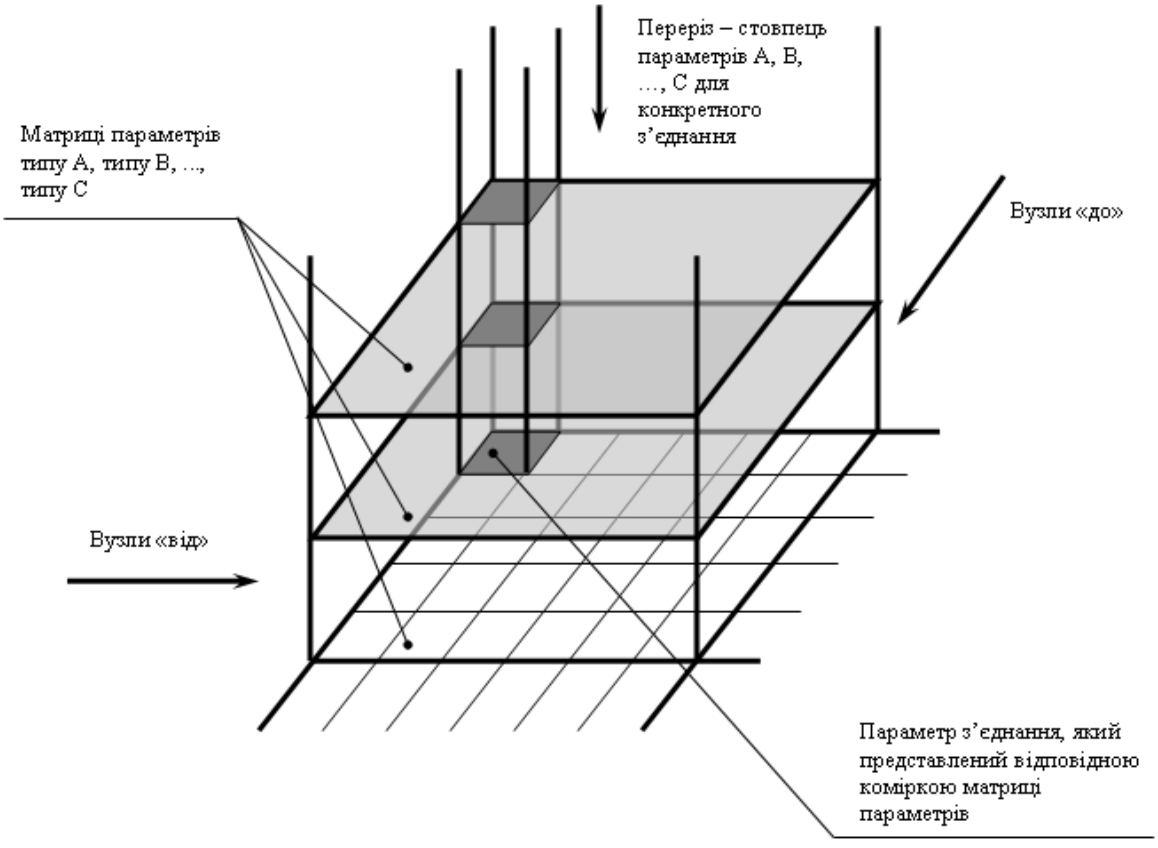
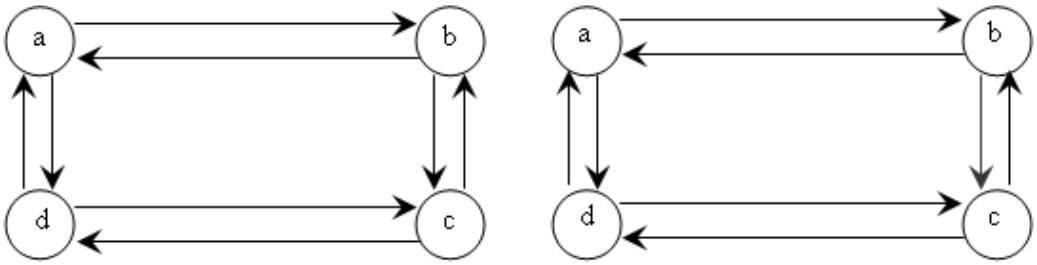


Рис. 2. Модель даних для дослідження структурної надійності мережі



а) *б)*

Рис. 3. Структурна схема мережі:
а – нормальний режим; б – режим аварії

Побудуємо так звану *матрицю доступних з'єднань*, тобто *матрицю суміжностей*, для випадків, коли мережа перебуває в нормальному режимі та режимі аварії. Матриця доступних з'єднань – це матриця, у комірках якої знаходиться 1 або 0, залежно від того, чи є з'єднання між вузлами, чи ж його немає. Ще однією особливістю матриць параметрів є те, що вони мають так звану напрямленість, тобто по вертикалі ми відкладаємо вузли, з яких виходить цифровий потік, а по горизонталі – вузли, в які цей потік відповідно входить. Отже, для випадків а) і б) відповідно маємо:

	a	**b**	**c**	**d**
a	1	1	0	1
b	1	1	1	1
c	0	1	1	0
d	1	0	1	1

	a	**b**	**c**	**d**
a	1	1	0	1
b	1	1	0	1
c	0	1	1	0
d	1	0	1	1

Як бачимо із другої матриці, з'єднання [b-c] стало недоступним і відповідно на перетині b-c маємо комірку із значенням 0.

Матриця доступних зв'язків постійно сканується *алгоритмом виявлення асиметричності*, який полягає ось у чому: почергово зчитується інформація з комірки [i,j] і порівнюється із значеннями [j,i], якщо вони не збігаються, то система генерує повідомлення, що з'єднання N[i]-N[j] недоступне, де N – вектор-рядок вузлів мережі. Це повідомлення перехоплює, наприклад, алгоритм пошуку резервного шляху, залежно від того, який тип резервування використовується. Дані про використані типи резервувань містяться у *матриці резервувань*, комірки якої містять інформацію про наявні (задіяні) механізми резервувань. Відповідно до конкретного механізму резервування алгоритм пошуку резервного шляху може звернутися до матриці резервних ресурсів, яка містить інформацію про наявні резервні ресурси (канали, волокна, "гарячий резерв" тощо).

Захист та резервування розподілених інформаційних систем

Потужність обчислювальних ресурсів в усьому світі зростає неймовірними темпами. Людство з головою занурилось у всебічне використання обчислювальної техніки. За останні 10 років у світі було накопичено і оброблено інформації в мільйони разів більше, ніж за весь попередній період його розвитку. Разом зі збільшенням обсягів накопиченої інформації зростає і потреба у потужних обчислювальних системах, здатних її обробляти.

Завдяки розвитку мережевих технологій ця проблема отримала ефективне вирішення – створення розподілених інформаційних систем, які являють собою інтеграцію обчислювального процесу на фізично розподілених інформаційних ресурсах. Під поняттям *інтеграція* у цьому випадку розуміють об'єднання вузлів обробки інформації в єдину обчислювальну систему для розв'язання певної задачі.

З точки зору надійності розподілену інформаційну систему можна умовно розглядати як мережу, тобто елементарними об'єктами у нас знову ж таки будуть вузли обробки інформації та з'єднання між ними, проте цього разу врахуємо багато відмінностей.

По-перше, у разі аналізу надійності розподіленої інформаційної системи не береться до уваги те, яким шляхом (тобто маршрутом) передається інформація між вузлами. Важливию є лише наявність з'єднання між вузлами, і якщо з'єднання із вузлом відсутнє, тоді такий вузол автоматично вважається неробочим.

По-друге, практично завжди розподілені інформаційні системи містять в собі так звані керуючі вузли. Основне їх завдання – це розподіл навантаження, що поступає на обчислювальну систему між її вузлами. Навантаженням на інформаційну систему може бути потік запитів користувачів, якщо ми маємо систему масового обслуговування, потік елементарних задач, якщо система використовується, наприклад, для розв'язування громіздких обчислювальних задач (рис. 4).

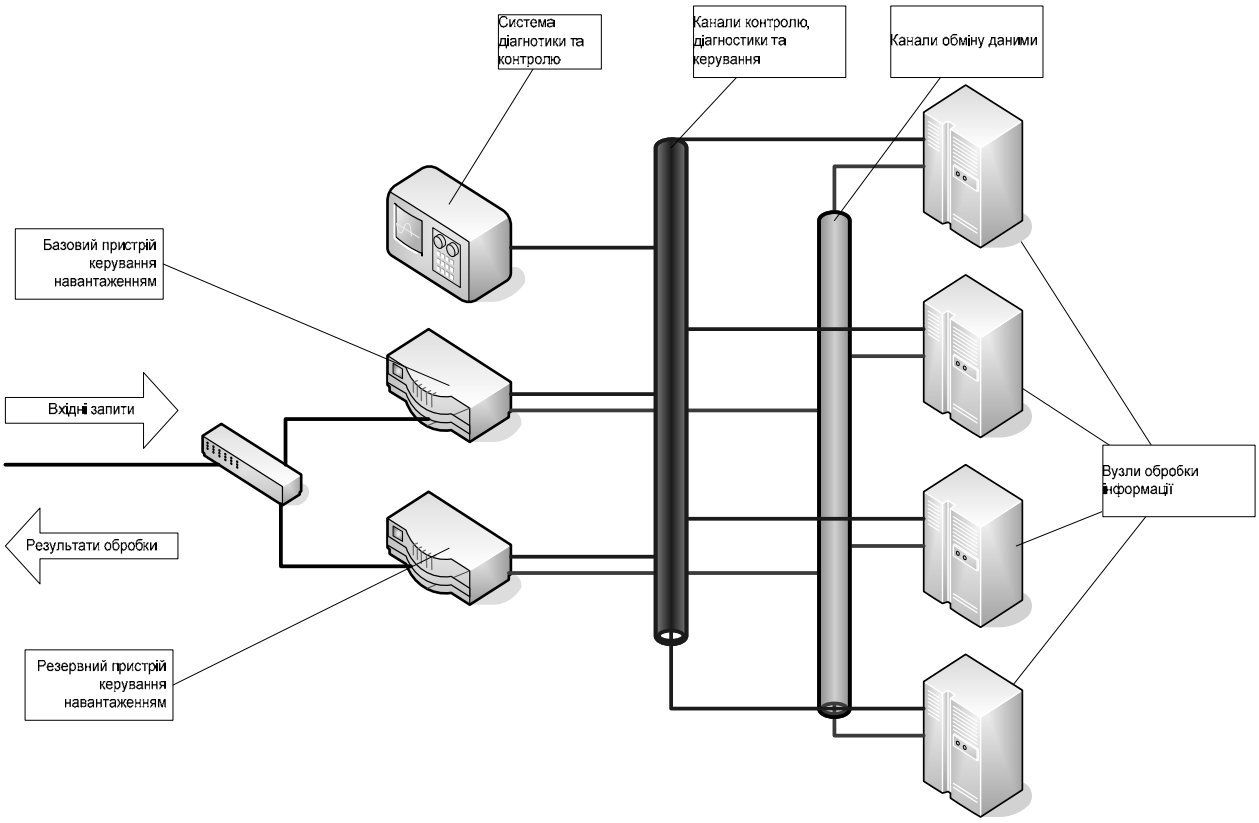


Рис. 4. Типова схема розподіленої інформаційної системи

Для аналізу розподілених обчислювальних систем також можна застосувати багатошарове матричне подання. Очевидно, що матриця суміжностей матиме вигляд одиничної матриці, наявною також буде матриця доступності вузлів, а також інші матричні дані. Слід зауважити, що на відміну від мережі, яку ми розглядали, і в якій усі вузли були одноранговим, розподілена обчислювальна система містить вузли різних рангів та пріоритетів, що відповідно вимагатиме створення так званої матриці рангів вузлів.

Щодо алгоритмів, то основний із них це є алгоритм розподілу навантаження між обчислювальними вузлами, що, як правило, ґрунтується на таких підзадачах, як пошук найменш завантаженого вузла, моніторингу доступності вузлів, залучення та вивільнення резервних ресурсів у разі переходу системи в аварійний режим роботи, і навпаки.

Розробка програмної моделі системи захисту та резервування інформаційної системи

Програмна модель системи захисту повинна забезпечувати:

- зручний інтерфейс користувача, що дав би змогу користувачеві нескладно та наочно задати топологію мережі чи архітектуру інформаційної системи, а також основні параметри її елементів, певні аналітичні залежності тощо;

• базу даних, в якій зберігається інформація про досліджувані мережі, загальна база даних обладнання, топологічних елементів тощо;

• виділену (*standalone*) бібліотеку функцій та класів, які б інкапсулювали увесь математичний апарат досліджень і могли б бути використані в інших програмних продуктах;

• зручний інтерфейс подання результатів дослідження: графіки, діаграми, звіти тощо.

На основі методу мультишарового матричного подання було розроблено комп'ютерну програму ***SDH NetAnalyzer***, яка дає змогу провести аналіз мережі, топологія чи архітектура якої задається користувачем.

Висновки

Розробка імітаційної моделі системи захисту та резервування ресурсів інформаційної вимагає насамперед створення ефективних математичних моделей та алгоритмів для подальшої їх реалізації, а сама наявність такої моделі дає змогу провести якісне дослідження та розрахунок системи захисту мережі під час її проектування чи аналізу.

Сьогодні, в умовах жорсткої конкуренції на ринку інформаційних послуг, поняття "бути завжди на зв'язку" має неабияке значення. Компанія-постачальник може провести тестування структурної надійності своєї існуючої мережі чи дата-центру за допомогою розробленого програмного забезпечення, що, своєю чергою, ґрунтується на описаних у цій роботі моделях досліджень, і в такий спосіб уникнути прямих збитків внаслідок штрафних санкцій з боку користувачів за недотримання умов договору про надання послуг доступу до інформаційних мереж та якості надаваного сервісу.

1. Vasseur Jean-Philippe, Pickavet Mario, Demeester Piet. Network Recovery: Protection and Restoration of Optical, SONET-SDH, IP, and MPLS., 2004, San Francisco. 2. Papadimitriou C., Steiglitz K. Combinatorial optimization: Algorithms and complexity. – Dover, Mineola, NY, 1998. 3. Microsoft Developers Network / MSDN. October 2005, Microsoft Corporation. http://msdn.microsoft.com/ library/default.asp. 4. Ефективні кластерні рішення. Компанія "Юстар". http://www.ustar.ua/section/ publication/ performance/1.html.

УДК 621.372

О.В. Тимченко, Р.С. Колодій
Національний університет "Львівська політехніка",
кафедра телекомунікацій

ПОРІВНЯННЯ МЕТОДІВ ОЦІНКИ ЯКОСТІ КОДЕРІВ МОВНОГО СИГНАЛУ ДЛЯ VoIP

Суб'єктивні випробування якості отриманого мовного сигналу дають можливість безпосередньо визначити, який рівень якості розмови є під час випробовувань реального або модельованого трафіку IP мережі. Вона прямо пов'язана з точкою зору споживача. Проте такі випробовування не є ефективні для оцінки, контролю і прогнозу дійсного кодера VoIP. Порівняно з ними об'єктивні вимірювання дають майже ті самі значення виміряної якості, в той самий час гарантуючи точність якісної оцінки.

Subjective test can directly derive which level the speech quality is from individuals who experience conversations or speech over real or model IP network traffic. It straight links to user's point of view. However, it is not efficient to evaluate, monitor and predict real VoIP coder. Compared to the shortcomings of subjective test, objective measurement can almost achieve those points, at the same time ensures the accuracy of quality assessment.

Вступ

Передавання аналогових сигналів є неможливе через мережі з комутацією пакетів, однією з яких є IP-мережа. Для здійснення такої передачі необхідно спочатку провести перетворення мовного сигналу до цифрового формату, закодувати його кодером та провести пакетизацію. Мережа, якою