
ВОЛОКОННО-ОПТИЧНІ ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНИХ (INTERNET, INTRANET ТОЩО) ТА ЕНЕРГЕТИЧНИХ МЕРЕЖАХ

УДК 004.75, 004.724.2

Г. В. ПОРЄВ

АРХІТЕКТУРНІ ЗАСАДИ РОЗПОДІЛЕНИХ ТА ОДНОРАНГОВИХ МЕРЕЖ

*Національний технічний університет
України «Київський політехнічний інститут»,
пр. Перемоги, 3703056, м.Київ, E-mail:core@barvinok.net*

Анотація. Виконано дослідження особливостей архітектури, а також специфіки застосування і перспектив розвитку однорангових і розподілених мереж.

Ключові слова: архітектура, дослідження, мережі, однорангові, розподілені

Аннотация. Проведены исследования особенностей архитектуры, а также специфики применения и перспектив развития одноранговых и распределённых сетей.

Ключевые слова: архитектура, исследования, сети, одноранговые, распределённые.

Abstract. The architectural specifics of peer-to-peer and distributed networks, as well as their development potential are evaluated.

Keywords: architecture, research, networks, peer-to-peer, distributed.

ВСТУП

В 1960-х роках обчислювальна потужність перших комп'ютерів досягла величин, які зменшили час виконання прикладних програм до рівня, що дозволив процесорам простоювати без роботи в очікуванні завантаження наступної програми. Це простоювання змусило розробників здійснити перші в історії галузі ІТ кроки в напрямку паралельної обробки інформації, і на початку 1970-х років з'явилися перші так звані «мейнфрейми» — комп'ютери з багатокористувацьким доступом. Доступ здійснювався за допомогою простих алфавітно-цифрових терміналів, процесорний час надавався всім користувачам по черзі, а зв'язок між терміналами та «мейнфреймом» здійснювався за допомогою паралельних інтерфейсів.

Таку схему можна вважати прообразом парадигми «клієнт-сервер», в рамках якої вузли комп'ютерної системи поділяються на сервери, які можуть надавати ресурси (обчислювальний час процесора, пам'ять тривалого зберігання (ПТЗ), послуги з'єднання тощо), клієнти, які споживають вказані ресурси та проміжне обладнання, яке здійснює передачу ресурсів або повідомлень про доступність даних.

Нетривалий період втрати цікавості ІТ індустрії до парадигми «клієнт-сервер» прийшовся на кінець 1980-х і початок 1990-х років завдяки масовому комерційному успіху персональних комп'ютерів, які дозволили кожному користувачу отримати окремий процесор у монопольне використання, навіть тоді, коли він простоює.

Але вже з появою комп'ютерних мереж взагалі і глобальних комп'ютерних мереж, зокрема, парадигма «клієнт-сервер» стала домінантною в мережах і до теперішнього часу, коли на ній базується переважна більшість інформаційних ресурсів мережі Інтернет.

В третьому тисячолітті Інтернет відіграє важливу роль як середовище для обміну та збереження даних. Протягом двох десятиліть постійного розвитку, технології Інтернет змінюються, вдосконалюються, стають застарілими та замінюються новими.

В той же час зміна базових архітектурних концепцій для Інтернет трапляється набагато рідше. Прикладом такої недавньої очевидної зміни є концепція однорангових мереж.

Однорангові мережі (P2P, peer-to-peer networks) визначають вузли, що беруть участь в роботі мережі як рівні, тобто такі, що знаходяться на одному рівні в їхньому відношенні і важливості. Кожний

вузол мережі може діяти як сервер для будь-якого іншого вузла в клієнтському контексті, і може діяти як клієнт, що потребує послуг від будь-якого іншого вузла в серверному контексті.

Крім того, зазвичай немає ніякої централізованої або фіксованої маршрутизації ні між якою даною парою вузлів — вони з'єднуються безпосередньо кожний з кожним при необхідності.

Однорангові мережі є частинним випадком розподілених мереж, які визначаються, як мережі, в яких програми для обробки даних, дані та представлення результатів обробки знаходяться на різних вузлах. Поява розподілених мереж зумовлена тими самими причинами, що і поступова відмова від парадигми «клієнт-сервер», зокрема використання кінцевих користувачьких терміналів як частини процесу обробки та представлення даних та питаннями відмово стійкості шляхом надлишкового копіювання на географічно розділених вузлах.

ЗАГАЛЬНА ПОСТАНОВКА ПРОБЛЕМИ

Однорангова мережа за своїм визначенням є мережею спільного використання ресурсу. Специфіка однорангової мережі [1], зокрема виконання її вузлами серверних функцій при негарантованості підключення кожного вузла, накладає певні обмеження на типи ресурсів.

Надавати обчислювальні потужності в середовищі однорангової мережі, на наш погляд, недоцільно, тому що це потребує створення складних алгоритмів контролю, які будуть шукати баланс між кількістю навантажених однією і тією самою задачею вузлів і гарантуванням та забезпеченням доставки результатів обчислень до вузла-замовника.

Використовувати однорангову мережу для надання зв'язності з зовнішнім каналом може виявитися доречним тільки у вузькоспеціалізованих задачах [2], коли можна гарантувати гомогенність апаратно-програмного забезпечення мережі і коли об'єми даних і швидкості передачі несуттєво впливають на продуктивність мережі в цілому. Зрештою, залишається лише один тип ресурсу, який економічно доцільно (в термінах витрат на експлуатацію і ефективності мережі) використовувати як розподілений ресурс — ПТЗ. За своєю природою цей ресурс не є ресурсом монопольного і одноразового використання, як зв'язок і заданий обсяг обчислень. Крім того, тенденція розвитку ІТ-індустрії така, що з часом стають необхідні дедалі більші об'єми ПТЗ для нових задач. Природно, що переважна кількість сучасних однорангових мереж орієнтована саме на використання розподіленої ПТЗ, зокрема для файлового обміну, безпечного зберігання архівних даних тощо.

На відміну від однорангових мереж, які чітко визначені принципом суміщення клієнтських і серверних ролей, розподілені мережі можуть мати диференціацію таких ролей. В них можна виділити вузли з чітко серверними та чітко клієнтськими функціями. В розподілених мережах, так як і в однорангових, відсутня інфраструктура централізації, тобто вузол або група вузлів, яка контролює роботу всіх інших. Розподілені мережі також не мають гарантованих в будь-який час підключень. Технологічний перехід від централізованих комп'ютерних мереж до розподілених має багато спільного зі зміною парадигми комп'ютерних мереж від «клієнт-сервер» до «однорангові мережі». Зокрема, це не була раптова і організована зміна технологій, але поступова еволюція засобів виробництва і керування в умовах, які були створені поставленими задачами. Метою даної роботи є дослідження особливостей архітектури та специфіки і перспектив застосування однорангових і розподілених мереж.

ПРОБЛЕМИ ВИКОРИСТАННЯ СТАНДАРТНИХ МЕТРИК ЧАСУ ВІДКЛИКУ ТА ТРАСУВАННЯ

Сучасні середовища моделювання та дослідження розподілених мереж не приділяють питанням визначення локальності суттєву увагу. Переважна більшість з них, коли мова йде про будь-яку метрику логічної відстані між вузлами мережі, використовує або затримку відклику, виміряну в одиницях часу, або кількість вузлів, які проходить пакет трасування (так званий засіб *traceroute*). Ці показники не тільки піддаються впливу непередбачуваних змін в умовах та якості каналів зв'язку, але вони потребують залучення додаткового вимірювального трафіку, а також суттєвого часу на проведення вимірювань.

Обраний для трасування протокол може бути відфільтрований на пограничних маршрутизаторах цільової системи, що унеможливить отримання результатів взагалі.

Коли мова йде про вимірювання часу відклику, зміна умов навантаженості каналів зв'язку може викликати збільшення часу відклику на порядок. В таких умовах, наприклад, не навантажений трафіком користувацький канал ADSL може відповісти швидше ніж повністю зайнятий гігабітний канал. Принцип роботи засобу трасування полягає в тому, що він відправляє послідовність пакетів на вказану цільову адресу, при цьому для кожної наступної групи пакетів значення поля TTL (*Time-to-live*) збільшується на 1, починаючи з першої групи, в якій це поле дорівнює 1. Кожний проміжний вузол повинен зменшувати значення цього поля перед передачею пакету далі. Коли значення поля досягає 0, таким вузлом у зворотному напрямку генерується службовий пакет з кодом помилки. Збільшення припиняється при досягненні цільового вузла або коли кількість проміжних вузлів перевищує задане значення, звичайно

30. Таким чином, при послідовному збільшенні значення TTL засіб отримує пакети з кодом помилки від кожного вузла, який приймає участь у передачі пакету.

Засоби трасування в залежності від платформи використовують три найбільш розповсюджених в мережі Інтернет протокола — TCP, UDP та ICMP. Вважається, що протокол ICMP є найбільш придатним для трасування, оскільки був спеціально розроблений як протокол керування передачею даних та діагностики мережі. Але специфіка інших функцій, які реалізуються протоколом ICMP та відсутність в ньому механізмів розподілення прав доступу призводить до того, що ICMP часто буває відфільтрованим на пограничних маршрутизаторах. Тому на платформах, споріднених GNU/Linux, протоколом за замовчуванням для засобу трасування використовується UDP.

Автори роботи [3] розглядають цілий клас таких завад, як «перемикання трафіку» і намагаються вдосконалити засіб трасування таким чином, щоб уникати негативних ефектів від даного класу завад при визначенні локальності.

Вказується, що схеми балансування трафіку в магістральних каналах застосовують автоматичне розподілення вхідного пакету даних на один з декількох вихідних інтерфейсів за певним алгоритмом. Це може бути циклічний перебір, явно вказані пріоритети. Найчастіше використовується маркування — призначення однакового маркера певному класу пакетів за ознаками, що вказані в його заголовку, наприклад, номери послідовностей, номери протоколів, групи вихідних або вхідних адрес тощо. В схемах балансування таке перемикання трафіку є суттєвим технологічним прийомом. При балансуванні кожного окремого пакету його маркери призначаються незалежно від інших, а у випадках балансування потоків обчислення маркерів виконується таким чином, щоб зберігати однаковий маркер для кожного з'єднання TCP або сеансу обміну UDP. При цьому маркери навіть для однієї і тієї ж пари вихідної та цільової адрес будуть різними, оскільки можуть відрізнятися номери протоколів, номери портів, ідентифікатори сеансу та послідовності тощо.

В [3] робиться висновок, що класичний засіб traceroute (програма командної оболонки, яка входить в стандартний пакет програм мережної діагностики як в ОС Windows, так і в ОС Linux) принципово не може знайти всі наявні канали зв'язку на тих ділянках проходження пакету, де присутнє балансування трафіку. Якщо ж маркерне перемикання каналів відбудеться безпосередньо під час вимірювань, то трасування може показати взагалі неіснуючий маршрут проходження пакетів (рис.1. та 2).

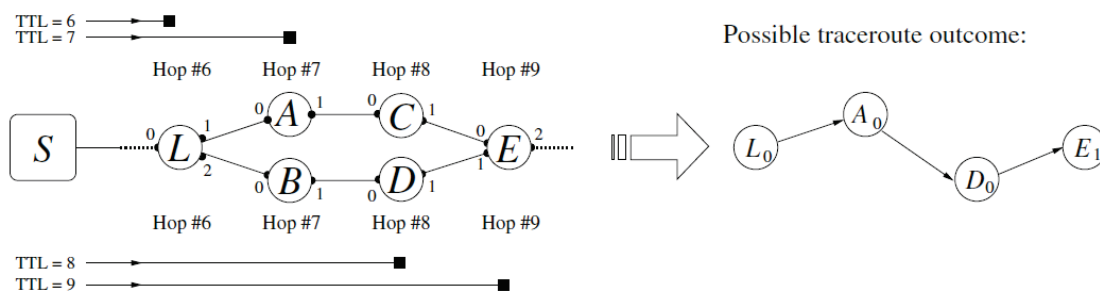


Рис.1. Типова ситуація перемикання трафіку та неіснуючий маршрут (L-A-D-E), знайдений засобом трасування [3]: S — вихідний вузол, L — вузол, де здійснюється балансування трафіку по двом маршрутам, A та C — вузли першого маршруту, B та D — вузли другого маршруту, E — кінцевий вузол ділянки балансування

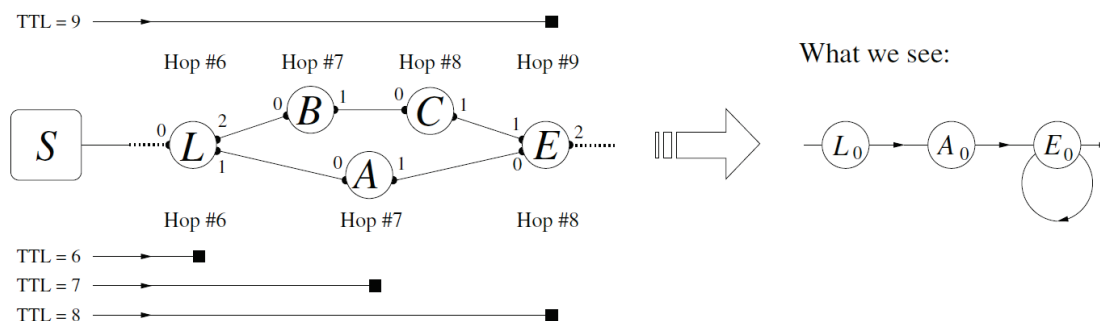


Рис.2. Типова ситуація перемикання трафіку та неіснуюча петля маршруту на вузлі «E», знайдена засобом трасування [3]: S — вихідний вузол, L — вузол, де здійснюється балансування трафіку по двом маршрутам, A та C — вузли першого маршруту, D — вузол другого маршруту, E — кінцевий вузол ділянки балансування

Для випадків, коли балансування трафіку виконується для потоків, автори роботи [3] створили вдосконалений засіб трасування Paris traceroute. В стандартних засобах трасування в залежності від обраного протоколу, заголовок кожного наступного пакета модифікується при зміні номеру послідовності ICMP або змісту UDP дейтаграми, відповідно змінюється і контрольна сума пакету. Paris traceroute підбирає змістовну частину пакету таким чином, щоб контрольна сума заголовку не змінювалася. Не змінюється також і номер послідовності, якщо таке поле передбачене поточним обраним протоколом. Таким чином алгоритми маркування потоків не призначають пакетам трасування різні маркери і пакети ідуть одним і тим самим шляхом.

Незважаючи на інноваційне рішення авторів вдосконаленого засобу трасування, експериментальні випробування [3] показали, що при отриманій підвищеній точності визначення топології ділянок маршруту передачі пакетів, цей метод все ще піддається артефактам трасування, таким як петлі, цикли та зорі з відносно високою частотою виникнення.

Крім того, Paris Traceroute потребує як мінімум такого ж часу, як і стандартний засіб трасування. В задачах академічного та дослідницького характеру це повністю припустимо, але як частина прикладного рішення для однорангових мереж з високим навантаженням по трафіку затримки тривалістю до хвилини можуть виявитися критичними для стабільної роботи. Навіть якщо кожен вузол зі списку опитування в одноранговій мережі буде опитано методом, запропонованим в [3] одночасно і паралельно, це все одно потребує до хвилини очікування і суттєвого обсягу службового трафіку. В ситуаціях, коли список опитування може модифікуватися в процесі роботи (як, наприклад, в файлообмінних мережах з великою кількістю джерел одиниці контенту), кожен новий вузол повинен буде пройти таку саму процедуру вимірювання топологічної метрики, що в умовах існуючого навантаження від вже запущених процесів обміну ще більше ускладнюється.

АРХІТЕКТУРНІ ВІДМІННОСТІ МІЖ РОЗПОДІЛЕНИМИ ТА ОДНОРАНГОВИМИ МЕРЕЖАМИ

Сьогодні дедалі частіше в роботах авторів, які займаються проблемами оптимізації функціонування розподілених мереж, зокрема однорангових, з'являються пропозиції, які можна умовно об'єднати під назвою «інфраструктура нагляд». Зокрема, в роботі [4], присвяченій розробці такої інфраструктури, робиться попередній висновок, що вузли однорангової мережі не мають технічної можливості повністю самостійно (без залучення зовнішніх джерел інформації) визначити топологію найближчої мережної околиці, дізнатися про правила та умови маршрутизації у операторів зв'язку тощо.

Так, наприклад, у операторів зв'язку з багатьма зовнішніми каналами зазвичай існує гнучка політика маршрутизації трафіку (т.з. reeving), коли шлях відправлення пакету вибирається в залежності від діючих ділових домовленостей бізнес-партнерів оператора, від поточного або планованого завантаження каналу тощо.

Автори роботи [4] приділяють особливу увагу питанню підвищення ефективності обміну трафіком однорангових мереж, між окремими сегментами Інтернет. Хоча це не вказано явно, мається на увазі ситуація, коли вузли однорангової мережі чи її окремої зрайки (підмножини вузлів мережі, які зайняті в обміні однієї опублікованої одиниці контенту) належать до адресного простору різних операторів зв'язку, різних автономних систем тощо. Прийнято вважати, що на сьогодні від 50% до 80% Інтернет трафіку в публічних мережах займає трафік однорангових мереж. Зазначається, що сучасні однорангові мережі мають достатньо високий ступінь самоорганізації для того, щоб самостійно і в егоїстичному режимі реагувати на зміни умов в каналах передачі даних. При спробі ІТ-персоналу оператора зв'язку впровадити систему динамічного врахування такого трафіку, система в цілому може перейти в режим осциляції в системі балансування, що погіршить якість надання послуги усім користувачам, а не тільки тим, які приймають участь в однорангових мережах.

Як тимчасове і досить непопулярне рішення цієї проблеми, деякі оператори зв'язку запроваджують вибіркочку фільтрацію передаваного трафіку на основі аналізу сигнатур даних, портів та тривалої динаміки встановлення вхідних та вихідних з'єднань. У відповідь виробники клієнтського ПЗ для однорангових мереж запровадили шифрування трафіку та принцип динамічного вибору портів.

Також автори роботи [4], роблять висновок, що ефективна оптимізація роботи однорангових мереж неможлива без оперативного врахування детальної інформації про стан каналів зв'язку. Для отримання та надання такої інформації пропонується ввести систему виділених служб, які організує кожен оператор зв'язку і які є доступними для клієнтів через спеціальний DNS-запит.

Такі служби, за задумом авторів, повинні зберігати оперативну інформацію про:

— локальність окремих заданих в запиті вузлів мережі по відношенню один до одного та до запитуваного вузла (також цей інтерфейс служби має надавати інформацію про топологічну прив'язку в контексті всієї мережі Інтернет, таку як номер автономної системи);

— систему внутрішніх технічних політик щодо маршрутизації трафіку, які визначаються

фінансовими, технічними або адміністративними аспектами роботи оператора зв'язку;

— підтримувані оператором додаткові можливості, наприклад, спеціалізовані класи маршрутизації, які можуть бути запитані клієнтами однорангових мереж, потокового мультимедіа тощо.

Схему запропонованої системи під назвою P4P (Provider Portal for P2P) зображено на рис.3.

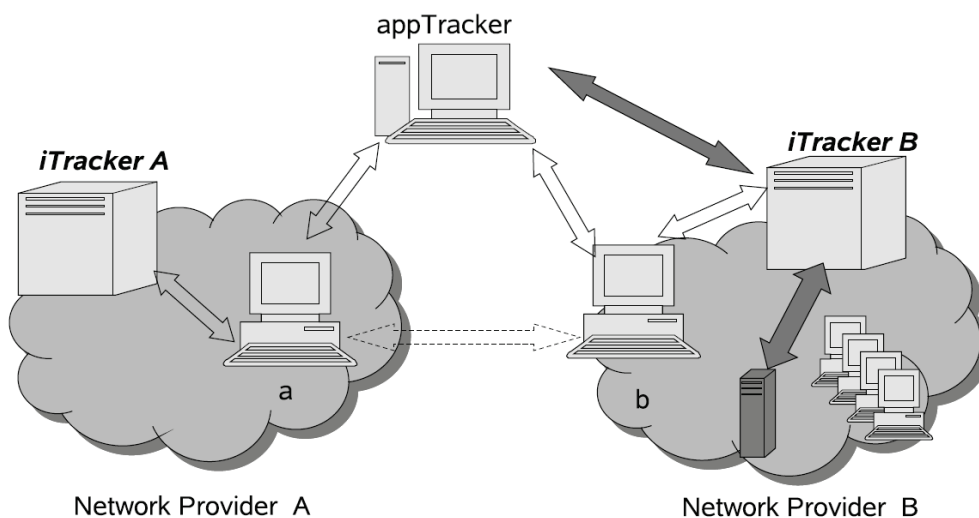


Рис. 3. Приклад взаємодії служб P4P [4] при обміні трафіку однорангової мережі між двома сегментами Інтернет: iTracker — виділені сервери, що реалізують інформаційний обмін за протоколами P4P, appTracker — координаційний сервер однорангової мережі, Network Provider — сегмент мережі Інтернет оператора зв'язку

Вузол, позначений як appTracker, не є складовою частиною системи P4P, і взагалі може бути відсутнім, якщо архітектура певної однорангової мережі не передбачає координаційних серверів.

Ключову роль в оптимізації в даному рішенні відіграють виділені сервери, що позначені на схемі як iTracker. Нехай в одноранговій мережі K зграйок. Кожний вузол зграйки отримує унікальний номер зграйки від трекара (appTracker), та повідомляє його iTracker, який слідкує за усіма зграйками в межах своєї точки присутності.

Позначимо вузли точки присутності (Point of Presence) як PoP-і. iTracker обчислює абстрактний граф $G=(V,E)$ з вузлами, які позначають PoP та гранями, що позначають канали зв'язку; збирає інформацію про стан мережі,

$$\begin{aligned} u_i^k &= \max\{\bar{u}_i^k - \bar{d}_i^k, 0\} \\ d_i^k &= \max\{\bar{d}_i^k - \bar{u}_i^k, 0\} \end{aligned} \quad (1)$$

iTracker періодично вирішує двохрівневу проблему оптимізації для формування вказівок вузлам однорангової мережі: балансування трафіку (тобто мінімізацію максимального використання каналу зв'язку) при максимізації швидкості передачі даних для кожної зграйки:

$$\min_{e \in E} \max \frac{b_e + \sum_k \sum_i \sum_{j \neq i} t_{ij}^k I_e(i, j)}{c_e} \quad (2)$$

Оновлені дані у вигляді переліку рекомендованих вузлів зі зграйки надсилаються за запитом інших вузлів з тієї самої зграйки. Автори роблять висновок, що таким чином зв'язки всередині зграйки будуть частіше локалізуватися в межах внутрішньої мережі одного оператора, де швидкість обміну може бути на порядок вища за швидкість зовнішнього каналу.

Схожу, але дещо складнішу схему (рис.4) пропонують автори роботи [5]. Вони використали розподілену науково-дослідну систему PlanetLab як базу для зовнішньої інфраструктури керування та знаходження мережної топології.

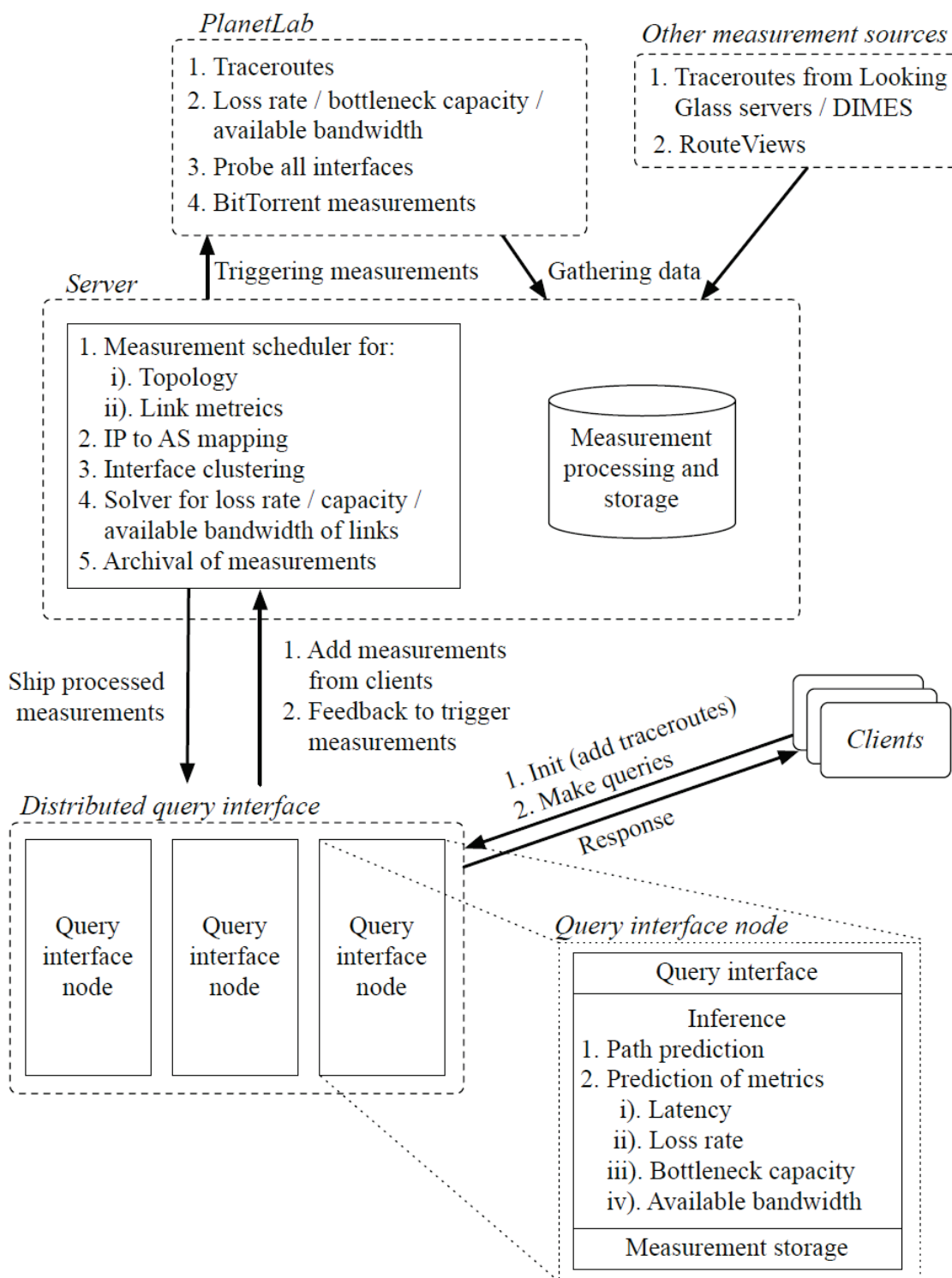


Рис.4. Функціональна схема мережі iPlane [5]: PlanetLab — джерело первинної інформації про поточні показники мережі, Other measurement sources — зовнішні джерела даних, Server — обчислювальне ядро системи iPlane, Distributed Query Interface — користувацький інтерфейс для клієнтів однорангової мережі

За допомогою модифікованих клієнтів однорангової мережі BitTorrent, система iPlane збирає та аналізує широкий спектр показників, які впливають і визначають ефективність та швидкість обміну даними. Зокрема, авторами розроблено так званий «алгоритм фронтиру» для визначення суттєвих в контексті певної однорангової мережі топологічних зв'язків та показників завантаження каналу.

Основою алгоритму є функція, вбудована в кожен клієнтський вузол однорангової мережі, яка

регулярно звітує до системи iPlane щодо маршруту, часу відклику вузлів при трасуванні з усіма вузлами, з якими даний вузол вступає в контакт та оціночного значення рівня втрати пакетів. iPlane згодом агрегує зібрану інформацію та обчислює узагальнену топологію актуальної частини мережі, а також оцінює ступінь завантаженості каналів в ній в цілому.

Крім того, система iPlane для спрощення обчислень топології виконує самостійну (без участі даних від поточних клієнтів мережі) кластеризацію мережі Інтернет на так звані «атоми», в ролі яких виступають в даному випадку префікси BGP, тобто стандартні одиниці множини правил маршрутизації. Дані отримуються за допомогою публічної служби RouteViews2, CoralReef3, служб типу «Looking Glass» та інших.

Серед усіх публікацій, в яких робляться спроби вирішити проблему локальності, авторами роботи [6] запропоновано спосіб, який розглянуто як вузькоспеціалізований по відношенню до мережі BitTorrent. В той же час авторами зауважено, що немає принципового протиріччя проти адаптації того ж методу під будь-який інший протокол обміну даними в одноранговій мережі, в якому передбачається запит на отримання частки збережених на іншому вузлі даних, тобто у файлообмінних мережах в першу чергу.

Автори проаналізованої вище роботи [6] розглядають систему доставки контенту на основі однорангових мереж як протиставлення традиційним системам доставки контенту на основі виділених корпоративних і географічно розподілених серверних ферм, але зауважують що різниця між цими принципами не є чіткою. На їх думку, певні елементи централізованого кешування можуть бути включені в процес обміну даними однорангової мережі, якщо вдається локалізувати певну частину трафіку всередині мережі оператора зв'язку.

Розглянемо технічне рішення, запропоноване авторами роботи [6] на основі даних тривалого аналізу трафіку BitTorrent (як запитів до трекера так і міжклієнтських зв'язків) та користуючись тим фактом, що протокол BitTorrent є відкритою специфікацією, пропонується використання проміжних автоматичних серверів кешування. Такі сервери повинні відслідковувати ідентифікатори всіх активних в мережі оператора клієнтів BitTorrent та всі заявлені ними ідентифікатори контенту (тобто участь вузлів у згайці), разом із бітовою картою доступності.

У випадку, якщо якийсь вузол А запитує частину контенту у іншого вузла В з тієї ж згайки, вузол В знаходиться за межами мережі оператора і в межах мережі оператора є вузол С, що приймає участь в тій самій згайці і має вже завантажену частину контенту, то такий сервер кешування здійснює прозору модифікацію трафіку таким чином, щоб замість вузла В вузол А встановив з'єднання з вузлом С.

Ця технологія зовні дещо нагадує прозору трансляцію адрес NAT. Оскільки вузли А та С знаходяться всередині мережі оператора, швидкість між ними майже завжди буде більше, а завантаження зовнішніх каналів оператора — менше. В роботі наводиться графік, що ілюструє вигоду від використання такої системи (рис. 5).

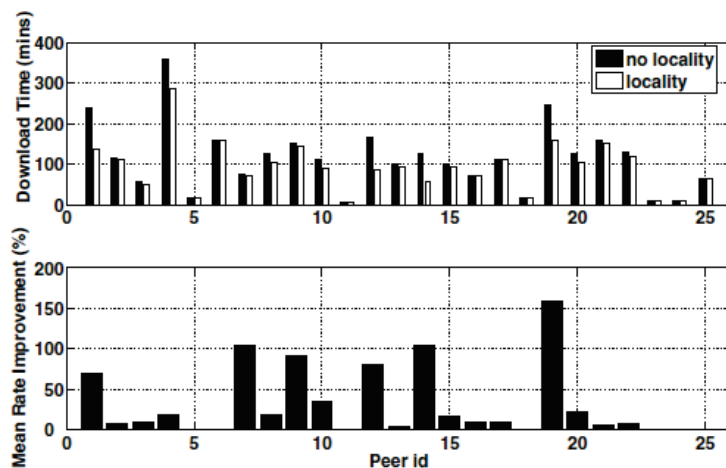


Рис.5. Порівняльні результати при використанні методу врахування локальності в BitTorrent: верхній графік показує час, витрачений 25 вузлами мережі в різних згайках на повне завантаження звичайним способом (чорний) і з врахуванням локальності (білий); нижній графік показує ті ж дані у вигляді відношення.

Фактично, такий сервер виконує функції BitTorrent-трекера, але на відміну від нього, він може втручатися в процес передачі даних навіть тоді, коли в згайці жодного справжнього трекера не передбачено. Подібно до того, як і деякі сучасні локальні «ре-трекери», такий сервер здійснює двохрівневе розрізнення локальності в контексті мережі оператора зв'язку.

В роботі [6] також вводиться спрощене поняття локальності, як показника завершеності завантаження контенту з згайки вузлами, що належать одній і тій самій мережі оператора зв'язку.

Зауважимо, що хоча автори роботи [6] і називають цей показник локальністю, він не має ніякого відношення до географічної або топологічної локальності та відображає лише відносну кількість вузлів з потрібними даними.

В даній роботі наведені далеко не всі розробки в цій галузі, а лише ті характерні, які виявляють тенденції в шляхах вирішення задач та проектуванні систем визначення локальності.

Як видно, велика частина таких робіт, присвячених оптимізації функціонування однорангових та розподілених мереж, так чи інакше розглядає певну зовнішню по відношенню до такої мережі інфраструктуру, яка виконує роль координатора.

Так, автори системи iPlane [5], створеної при організаційній підтримці консорціуму PlanetLab, пропонують використовувати ту саму мережу PlanetLab і для запуску повноцінної робочої версії системи iPlane в експлуатацію.

Розподілена науково-дослідницька мережа PlanetLab є власністю комерційного консорціуму освітянських та наукових установ, підприємств та організацій, основним полем діяльності яких є розвиток мережної інфраструктури та комунікацій. Умови приєднання до системи PlanetLab передбачають надання в повне користування системним адміністраторам консорціуму апаратних ресурсів, зокрема серверів та виділеного каналу в Інтернет, сконфігурованих певним чином.

Сторонні приватні користувачі та користувачі з організацій, що не входять до консорціуму, не мають доступу до ресурсів мережі. Рішення, автори яких вибирають в якості основної продуктивної платформи систему PlanetLab або іншу аналогічну систему, можуть поставити функціонування власних науково-дослідних розробок в залежність від комерційної та технологічної політики власників мережі.

Крім того, якщо автори таких розробок планують надавати публічний доступ до їх функціональності, потенційні користувачі виявляються у подвійній залежності — не тільки від політик консорціуму PlanetLab, від доброї волі авторів розробок як гарантії доступності потрібних служб на комерційних ресурсах, а і від людського фактору, який полягає в одночасній експлуатації вузлів системи PlanetLab і як продукційних, і як науково-дослідних, що може поставити під загрозу стабільність роботи кожного вузла.

В інших випадках, коли запропоновані рішення не базуються на вже існуючій і розвиненій розподіленій мережі, зовнішню інфраструктуру пропонується запровадити або як індустріальний стандарт, який змусить операторів зв'язку Інтернет встановлювати додаткові апаратно-програмні рішення в межах своїх сегментів мережі, або як опціональні служби [4].

Це, по-перше, означає матеріальну відповідальність за впровадження таких рішень і покладає її на кінцевих операторів зв'язку.

По-друге, це суперечить загальноприйнятій практиці стандартизації технологій Інтернет, коли галузевий стандарт приймається IETF (Internet Engineering Task Force) лише після того, як запропоноване рішення продемонструє свою реальну життєздатність на теренах мережі і матимуть широке розповсюдження принаймні дві незалежні але обов'язково сумісні між собою в рамках проекту, реалізації.

Також можна помітити, що в якості джерел даних для конструювання топології мережі та розподіленого визначення її параметрів використовуються приватні або академічні проекти, такі як згадані вище CoralReef та RouteViews, які не мають ніяких легальних зобов'язань перед потенційними користувачами їх функцій.

Всі перераховані вище недоліки є так званою «єдиною точкою відмови» (single point of failure), порушення нормальної роботи якої приводить до краху всієї системи. Порушення може мати як технічний характер (відключення або збій сервера, який надає послуги користувачам публічного доступу), так і адміністративний — зміна корпоративної політики консорціуму, яка приводить до припинення надання послуги, або припинення функціонування мережі, або втрата цікавості чи фінансової підтримки колективу дослідників з боку наукових фондів. Зрозуміло, що неприпустимо ставити публічну систему, яка розроблена для одночасного розгортання на сотнях тисяч вузлів по всьому світу, від такої єдиної точки відмови.

ВИСНОВКИ

З появою комп'ютерних мереж взагалі і глобальних комп'ютерних мереж, зокрема, парадигма «клієнт-сервер» стала домінантною, оскільки на ній базується переважна більшість інформаційних ресурсів мережі Інтернет.

Сучасні однорангові мережі мають достатньо високий ступінь самоорганізації для того, щоб самостійно реагувати на зміни умов в каналах передачі даних.

На відміну від однорангових мереж, які чітко визначені принципом суміщення клієнтських і серверних ролей, розподілені мережі можуть мати диференціацію таких ролей.

Надання обчислювальних потужностей в середовищі однорангової мережі потребує створення складних алгоритмів контролю, які будуть шукати баланс між кількістю навантажених однією і тією самою задачею вузлів і гарантуванням та забезпеченням доставки результатів обчислень до вузла-замовника.

Використання однорангової мережі для надання зв'язності з зовнішнім каналом може виявитися доречним у вузькоспеціалізованих задачах, коли можна гарантувати гомогенність апаратно-програмного

забезпечення мережі і коли об'єми даних і швидкості передачі несуттєво впливають на продуктивність мережі в цілому.

В статті використані матеріали, отримані при виконанні робіт по гранту президента України для підтримки наукових досліджень молодих вчених, НДР GP/F27-0040 «Дослідження регуляційних та рейтингових методів в однорангових мережах типу BitTorrent» договір № Ф27/8-2010 від 12 лютого 2010.

СПИСОК ЛІТЕРАТУРИ

1. Порєв Г. В. Архітектура комп'ютерних мереж. Методичний посібник. – Вінниця: Універсум-Вінниця, 2008. – 98 с.
2. Poryev G. On the application of peer-to-peer network architecture for global ecological information and monitoring systems / G. Poryev, V. Poryev // Тези доповіді Третьої науково-практичної конференції «Моніторинг навколишнього середовища: наукове, методичне, технічне та програмне забезпечення» / SEC-EST. – Коктебель: 2008. – С. 102.
3. Avoiding traceroute anomalies with paris traceroute / B. Augustin, X. Cuvellier, B. Orgogozo et al. // IMC '06: Proceedings of the 6th ACM SIGCOMM conference on Internet measurement. – New York, NY, USA: ACM, 2006. – Pp. 153–158.
4. Xie H. P4P: Explicit communications for cooperative control between P2P and network providers: [Електронний ресурс] / H. Xie, A. Krishnamurthy, A. Silberschatz, R.Y. Yang. – 2007. www.dcia.info/documents/P4P_Overview.pdf.
5. iPlane: An information plane for distributed services / H. Madhyastha, T. Isdal, M. Piatek, C. Dixon // In Proceedings of the 7th USENIX Symposium on Operating Systems Design and Implementation. – USENIX, 2006. – Pp. 367–380.
6. Karagiannis T., Rodriguez P., Papagiannaki K. Should internet service providers fear peer-assisted content distribution? // IMC '05: Proceedings of the 5th ACM-SIGCOMM conference on Internet measurement. – New York, NY, USA: ACM, 2005. – Pp. 63–76.

Надійшла до редакції 02.10.2010р.

ПОРЄВ ГЕННАДІЙ ВОЛОДИМИРОВИЧ – к.т.н., докторант НТУУ «Київський політехнічний інститут», Київ, Україна, тел.: (068) 321-345-1, E-mail: core@barvinok.net