

УДК 004.738 (045)

Лукашенко В.В., к.т.н.,
Новгородцев А.І.

ОГЛЯД І СПЕЦИФІКА ЗАСТОСУВАННЯ МЕРЕЖ DTN

Національний авіаційний університет

v.v.lukashenko@gmail.com

novgorodcevandrew@gmail.com

Розглянуто особливості архітектури мереж DTN. Визначено основні відмінності роботи протоколів від традиційних мереж. Наведено напрями застосування та приклади додатків

Ключові слова: мережа; толерантна до затримок; мережний протокол; затримка; нерегулярне з'єднання; періодичний зв'язок; космічний зв'язок; міжпланетний Інтернет

Вступ

Розвиток інформаційних, зокрема, мережних технологій та прагнення їх застосування в нових спеціальних галузях (дистанційний збір інформації у важкодоступних областях нашої планети, у космічному просторі тощо) призводить до появи різноманітних способів комунікації та створення мереж нового покоління.

Однією з таких є мережі, толерантні до затримок і частих розривів зв'язку (англ. Delay & Disruption-Tolerant Networking).

В даному випадку розглядаються не затримки, що спричинені транзитними вузлами чи впливом пропускну здатності каналу зв'язку. Додаткові затримки, які з'являються при передачі даних, не залежать від обсягу та швидкості передачі. Такі затримки породжуються довжиною пройденого сигналом шляху і швидкістю його поширення в середовищі передачі.

Концепція цієї архітектури лежить в основі міжпланетного Інтернету (IPN), що є проектом NASA і використовується для мереж наддалекого космічного зв'язку.

Окрім цього, основа даної архітектури закладена в роботу сенсорних мереж, які використовують підключення за розкладом, наземних бездротових мереж, що не можуть нормально підтримувати з'єднання точка-точка,

супутникових мереж з помірними затримками і періодичністю зв'язку, і підводних акустичних мереж з помірними затримками і частими перебоями, пов'язаними з факторами навколишнього середовища [1-2].

Однією з основних особливостей якості роботи комп'ютерної мережі є надійність передачі інформації по мережі, а саме, ймовірність доставки повідомлення до одержувача, час, за який це повідомлення буде доставлено, і рівнозначність відправленого та отриманого повідомлень.

Однак, існують ситуації, в яких показник ймовірності того, що повідомлення взагалі дійде до приймаючого пристрою, може прагнути до нуля. Так, наприклад, у випадку порушення або відсутності відповідної технічної інфраструктури сигнал просто не дійде до найближчого вузла комутації, як це може бути у випадку природних чи техногенних катастроф [3].

Постановка проблеми

В одній з найважливіших для людства космічній галузі в даний час дуже істотною проблемою є збільшений час відгуку сигналу, яке спостерігається при сеансах міжпланетного та супутникового зв'язку. Наприклад, у випадку передачі сигналу на орбітальні станції інших об'єктів Сонячної системи час затримки може досягати декількох

годин. Сигнал із Землі до Марсу йде декілька хвилин, зворотний шлях займе ще стільки ж. До того ж, потрібно ще враховувати обертання планети. Якщо намагатися встановити зв'язок з чимось, що знаходяться на поверхні, то після того як планета повернеться, ця можливість буде втрачена, і доведеться чекати, поки вона не зробить повний оберт. Окрім затримок, проблема посилюється підвищенням кількості спотворених даних через перешкоди, викликані зовнішніми факторами, зокрема, перекриття шляху сигналу космічними об'єктами невеликого розміру, сонячна активність і таке інше[4].

Не викликає сумніву той факт, що надійність забезпечення наддалекого космічного зв'язку є дуже актуальною в даний час. Навіть якщо розглядати таку знайому всім область як використання мобільного зв'язку, то і в цьому випадку також в сучасних комунікаційних мережах мобільної телефонії часто зустрічаються ситуації, при яких стає неможливим передавати інформацію в мережі. Наприклад, у випадку великого завантаження базової станції мобільної мережі і перевищенні максимально допустимого (критичного) часу відгуку виконання запитів до сервера виявляється проблематичним. Щоб змінити ситуацію в кращу сторону було безліч спроб розробити нові протоколи (правила передачі даних у мережі), так як існуючі традиційні протоколи з таким завданням не справляються. Передача даних може взагалі не відбутися, і повідомлення може не бути отримано в силу особливостей існуючих протоколів.

Проблемам розробки, дослідження теорії та практики, механізмів і протоколів архітектури DTN мереж присвячені фундаментальні праці В. Серфа, С. Барлі, Р. Даста, К. Фолла, Е. Хука, К. Скотта, Л. Торджесена, Г. Вайса.

Питання збіжності протоколів даних мереж з Інтернет протоколами розглядалися і вирішувалися у працях таких науковців і практиків, як М. Дж.

Деммер, Дж. Отт, С. Пероу.

Розробкою протоколів безпеки передавання даних через DTN мережі займалися С. Симигтон, С. Фаррел, Г. Вайс, П. Ловелл, М. Рамадас.

Проте в практичному відношенні залишається невирішеною проблема розробки ефективного протоколу маршрутизації через дані мережі. Дану проблему досліджували у своїх наукових працях К. Фолл, С. Джейн, Р. Патра, Дж. Алонсо, Дж. Леґуа, Т. Фрідман, В. Конан.

Мета дослідження

Метою дослідження є проведення огляду толерантних до затримок мереж, проаналізувати їх перспективність. Виявити актуальні питання і проблеми.

DTN і їх протоколи

В даний час сценарій роботи традиційних протоколів для роботи мереж базується на певних припущеннях. Так, одним з головних припущень, що лежать в основі стандартного протоколу для комп'ютерних мереж TCP / IP, є те, що часи затримки на всьому протязі шляху пакета від джерела до місця призначення невеликі. Для встановлення з'єднання в протоколі TCP використовується правило «тристороннього рукостискання»: час встановлення з'єднання пропорційний значенню часу затримки пакету в мережі. Але якщо затримки часу є достатньо великими, то, наприклад, звичайний веб-браузер, як правило, видає повідомлення типу «інформація не зможе бути отримана користувачем або сервер не знайдено». Крім того, слід зауважити, що перед відправкою пакета в традиційних мережах необхідно здійснювати перетворення адреси з доменного імені в IP-адресу, а потім з IP-адреси в MAC-адресу. Таке перетворення припускає наявність відповідної інфраструктури, а саме: певних DNS-серверів, маршрутизаторів, шлюзів і т.д. Якщо така інфраструктура відсутня, працездатність мережі буде порушена практично на всіх рівнях моделі взаємодії відкритих систем, починаючи з відсутності зв'язку на фізичному рівні і

закінчуючи неможливістю роботи програм на верхньому рівні. Через великі затримки замість IP адресації і системи DNS використовують уніфіковані ідентифікатори ресурсів.

Отже, існуючі протоколи Інтернету працюють не дуже добре в деяких середовищах, через вбудовані в них фундаментальні припущення:

- шлях з кінця в кінець між джерелом і адресатом існує на період тривалості сеансу зв'язку;
- повторні передачі лежать в основі своєчасного і стабільного зворотного зв'язку від одержувачів даних, що є ефективним засобом для виправлення помилок передачі;
- втрати є відносно невеликими;
- всі маршрутизатори і кінцеві станції підтримують протоколи TCP / IP;
- програмам верхнього рівня не потрібно турбуватися про надійність передачі;
- механізм безпеки, реалізований на кінцевих вузлах, достатній для вирішення більшості проблем;
- пакетна комутація є найбільш підходящою для сумісності і продуктивності;
- вибір одного маршруту між відправником та одержувачем достатній для досягнення прийнятної продуктивності зв'язку.

Архітектура DTN задумана, щоб відійти від більшості з цих припущень, на основі ряду принципів проектування:

- використання змінної довжини (можливо довгі) повідомлення (не потоки або пакети обмеженого розміру) як абстракцій зв'язку, щоб допомогти підвищити здатність мережі до планування або вибору шляху, коли це можливо;
- використовується синтаксис імен, який підтримує широкий спектр імен та адресних конвенцій для підвищення сумісності;
- використання сховища в мережі, щоб підтримувати операції зберігання і передавання по декільком шляхам і

протягом потенційно тривалих періодів часу (підтримка роботи в середовищах, де може бути багато шляхів або жодного шляху від відправника до одержувача), тобто не вимагається існування повного шляху між джерелом і адресатом;

- забезпечення механізмів безпеки, які захищають інфраструктуру від несанкціонованого використання, шляхом відкидання трафіку якомога швидше;
- забезпечення класів обслуговування, варіантів доставки і способу відображати корисний термін служби даних, дозволяє мережі краще передавати дані для задоволення потреб [1].

Таким чином для вирішення проблем TCP/IP протоколів в мережах з великими затримками при передачі повідомлень розроблені нові протоколи для архітектури DTN [5]. Дані протоколи засновані на парадигмі «зберігати дані і перенаправляти їх далі». Ці протоколи оперують спеціальними одиницями інформації – bundle (англ. повідомлення, пучок). По суті, bundle — це повідомлення, що містить в собі, поряд зі значимим для докладання вмістом, також і необхідну для маршрутизації інформацію. Вузли DTN, обмінюючись повідомленнями bundle, зберігають їх. У міру появи зв'язку з наступним вузлом даний bundle пересилається далі, поки не буде досягнутий вузол призначення або час життя bundle закінчиться.

Bundle Protocol (BP) працює між прикладним і транспортним рівнями моделі взаємодії відкритих систем і координує роботу режиму операцій зберігання і передавання. Для передавання використовує місцеві для мережі протоколи, в якій він працює.

Інтерфейс між BP і набором міжмережних протоколів називається рівнем конвергенції. На цьому рівні працює протокол LTP (Licklider transmission protocol), який також називають longhaul (далекомагістральний) transmission protocol. LTP робить автоматичний запит повторної передачі

даних шляхом вибіркового отримання звіту про прийом. Він стабільний і не має ніяких узгоджень або рукостискань. LTP призначений для забезпечення надійності заснованої на повторній передачі через канали зв'язку, що характеризуються надзвичайно великим часом прийому і передачі повідомлення в обидва кінці та/або частими перервами у зв'язку. Зв'язок по міжпланетному простору є найбільш яскравим прикладом такого зв'язку. LTP принципово спрямований на підтримку далекомагістральної надійної передачі в міжпланетному просторі, але має застосування в інших середовищах [1, 6-7].

Спочатку архітектура DTN була задумана як «Міжпланетний Інтернет», а в даний момент являє собою набір протоколів для мереж з великим часом затримки сигналу і отримує все більше застосування. Оскільки традиційний протокол передачі даних прикладного рівня за семи рівнями моделі OSI не може вирішити виникаючі в нових умовах проблеми, тобто працювати в DTN мережах через свої особливості, такі як численні пари «запит-відповідь». Отже, виникає необхідність у частковій модифікації програм і протоколів прикладного рівня для роботи в мережах DTN. Протоколи DTN істотно відрізняються від звичних протоколів (наприклад, TCP або UDP). При цьому поточний стан каналу зв'язку не впливає на доставку даних. Для вищезгаданих протоколів при неможливості доставки даних, в момент їх передачі, вони видаляються. В основі роботи архітектури DTN мереж лежить принцип збереження і передачі: «Store and Forward» [3].

Основний сервіс рівня bundle являє собою негарантовану доставку одноадресного повідомлення з пріоритетом та без підтвердження. У якості опцій підтримуються підтвердження доставки та передавання з опікою. Якщо додатки самостійно «бажають» контролювати передачу даних, така можливість надається.

Передача повідомлення з опцією опіки включає в себе передачу разом з повідомленням відповідальності за надійну доставку між вузлами DTN по мережі. Вузли, які отримали повідомлення і згодні взяти відповідальність за його надійну передачу, називаються опікунами або хранителями. Якщо додатку не потрібна передача з опікою, то механізм надійної передачі покладено на протоколи нижніх рівнів. Якщо додаток дав запит на передачу з опікою, а сусід не може надати дану послугу, то повідомлення може бути передано через декілька вузлів DTN перш ніж знайде хранителя. Для сусіда запит на передачу з опікою носить рекомендаційний характер. Період зберігання або час життя даних, маршрутна інформація, клас обслуговування вказані у службовому блоці повідомлення. Вводиться механізм для видалення застарілих даних. Використовуються черги для класів обслуговування. Дані з вищим пріоритетом будуть відправлені раніше, але різні черги для кожного вузла призначення [1, 6]. Оскільки взаємодія може відбуватися між додатками з різних типів мереж, для забезпечення безпеки даних при передачі через мережі DTN були розроблені сервіси для BP. Є чотири типи блоків безпеки, які можуть бути включені в повідомлення. Це блок аутентифікації повідомлення, блок цілісності, блок конфіденційності і блок розширеної безпеки [8].

Таким чином, якщо в якийсь проміжок часу не має маршруту для передачі даних на вузол призначення або проміжний вузол, дані зберігаються. Після відновлення зв'язку дані передаються далі. Одночасно з розробкою подібних протоколів постає проблема оцінки надійності та якості роботи такої мережі. Тому моделі надійності для мереж, що працюють на традиційному протоколі TCP, у випадку DTN мережі, не підходять. Крім того, при збереженні апаратної частини комп'ютерної мережі

при переході на протокол DTN зміниться сегмент транспортної мережі, що відповідає за технологію передачі даних.

Для вирішення питання збіжності стеку протоколів TCP/IP і протоколів DTN був запропонований TCP-based convergence-layer protocol (TCPCL). TCPCL - це протокол DTN, що працює на рівні конвергенції прикладного рівня, для

взаємодії BP і TCP протоколів [9]. IBR-DTN (iterated best response-DTN) – програмна платформа для додатків DTN, забезпечує інтерфейс програмного забезпечення для обміну даних і їх маршрутизації [4].

На рис. 1 представлено положення BP протоколу і рівня конвергенції в моделі TCP/IP [9].

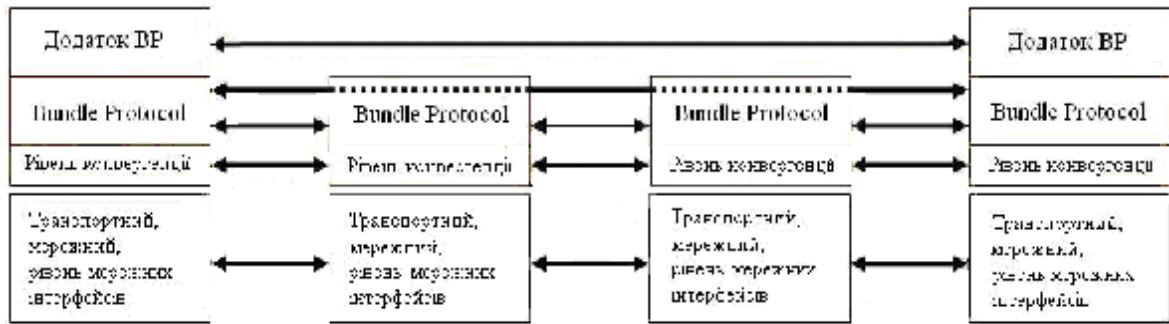


Рис.1 Положення BP протоколу і рівня конвергенції в моделі TCP/IP.

Маршрутизація в DTN.

Протоколи маршрутизації, в залежності від того, коли обчислюється маршрут, поділяються на проактивні, реактивні та гібридні.

Проактивні протоколи, які ще називають превентивними, табличним або активно-адаптивними, з початку своєї роботи на основі топології мережі формують повну таблицю маршрутизації. Такий підхід використовують протоколи в мережах з надійним постійним зв'язком.

Реактивні протоколи, які ще називають протоколи за вимогою або пасивно-адаптивні, починають пошук маршруту при наявності даних для передачі. Даний підхід реалізується на алгоритмі повені, при якому перший пакет даних або службовий пакет протоколу відправляється усім сусідам. Вони в свою чергу – своїм сусідам і так далі, доки пакет не дійде до вузла призначення. Маршрут з найменшою кількістю проміжних вузлів фіксується у вигляді переліку здійснених вузлів від відправника до призначення. В даному випадку необхідно враховувати затримку на обчислення маршруту при першій передачі.

Гібридні протоколи використовують поєднання проактивного і реактивного підходів[4,10].

За принципом передачі даних існуючі протоколи маршрутизації можна поділити на[11]:

- протоколи односпрямованого пересилання, в яких трафік прямує від вузла відправника до вузла призначення;
- протоколи ширококомовного пересилання, в яких трафік отримують всі вузли;
- протоколи гібридного підходу, в яких трафік отримує певна кількість вузлів.

Протоколи односпрямованого пересилання використовуються у випадках повної інформації про топологію і стан мережі.

Протоколи ширококомовного пересилання використовуються при відсутності або мінімуму інформації про топологію мережі. Можуть бути корисними у випадках неможливості повторної передачі даних. В якості недоліку даного типу можна вказати велику кількість копій одних даних в мережі[4].

Період зв'язку між вузлами

називають контактом. Розрізняють основні види контактів [1]:

- постійні – доступні постійно, наприклад з'єднання мережі Інтернет;
- за вимогою - з'єднання, що встановлюються за вимогою однієї з сторін, наприклад dial-up;
- переривчасті за розкладом - з'єднання, що встановлюються за певним розкладом, наприклад зв'язок з низькоорбітальним супутником;
- переривчасті випадкові – неочікувані з'єднання, наприклад зв'язок між електронним пристроєм клієнта і точкою доступу Wi-Fi кав'ярні;
- переривчасті прогнозовані - здійснюються на основі прогнозу, що спирається на історію попередніх з'єднань.

В перших двох видах контактів, якщо затримки відносно невеликі, можуть використовуватись традиційні протоколи маршрутизації.

Пошук маршруту в останніх трьох видах контактів залишається активно досліджуваною галуззю. Окрім великих затримок і не існування всього шляху від відправника до вузла призначення, проблема ускладнюється випадковістю контактів. Тому для вирішення питання пошуку маршруту в цих мережах необхідні протоколи, робота яких буде опиратися на прогноз або розклад з'єднань[1]. Для вибору найкращого маршруту при роботі традиційних протоколів в основному використовуються дані про пропускну здатність каналу та кількість проміжних вузлів[11]. В DTN мережах, окрім цього, для вибору маршруту необхідно враховувати набагато більше різних факторів, наприклад імовірний час та період контакту, завантаженість сусідів, їх об'єм вільної пам'яті для зберігання даних та час роботи від джерела живлення [4, 12].

DTN-додатки

У якості DTN додатків можуть бути програми веб-кешування, електронна

пошта, програми для пішохідних туристів, програми передачі метеорологічних даних, програми відстеження тварин та ін..

Програми веб-кешування дозволяють користувачам DTN отримати всю необхідну інформацію від певної веб-сторінки або групи сторінок за допомогою одного запиту до шлюзу в Інтернеті. Їх мета зробити цю операцію якомога більше прозорою для користувача за допомогою стандартного веб-браузера, навіть якщо синхронний пошук інформації не є можливим, і що система не має змоги доставити достатню кількість інформації для відображення сторінки або сторінок з одного повідомлення інформації, який повертатимуть через DTN. Це реалізуватиме модель «поштовх», в якій пучки інформації можуть бути про-активно доставлені шлюзами в межах DTN, по мережі, або регулярно за розкладом (наприклад, для передачі інформації новин на щоденній основі) або в результаті дій користувача.

Програми для роботи зі звичайною електронною поштою тільки адаптовані до архітектури DTN. Ці програми мають відправляти і отримувати електронну пошту в/з DTN регіонів, а також в/з джерел електронної пошти, що можуть бути розташовані в загальній мережі Інтернет.

Програми для пішохідних туристів, що мають допомагати користувачам DTN (наприклад туристам і дослідникам) по деяким послугам, наприклад дані аварійно-рятувальні служб, точок інтересу, медичних або фізичних послуг, повинні відсилати дані про своє місцезнаходження, завантажувати карти, що відносяться до даної місцевості, коли є можливість підключення.

Програми передачі метеорологічних даних використовуються як на підтримку сучасних заходів в сільських районах, у тому числі скотарства і екотуризму, так і моніторинг середовища в районах, де збір даних є переривчастий або неіснуючим. Також є необхідність у зборі екологічних

даних з усіх регіонів земної кулі і для надання допомоги в прогнозуванні погоди та моніторингу більш довгострокових наслідків на глобальний клімат.

Програми відстеження тварин призначені для моніторингу наземних і морських популяцій диких тварин. Наприклад, для відстеження економічно важливих видів в Арктиці, зокрема, в оленячих стадах, що являються основою традиційної господарської діяльності в регіоні Лапландії, які можуть вільно переміщатися по дуже великих площах. Основною метою такої програми є надання економічно ефективного способу контролювати розташування окремих тварин [13].

Висновки

В даній статті проведено огляд особливостей архітектури мереж DTN, основних відмінностей роботи протоколів від традиційних мереж. Наведено напрями застосування та приклади додатків. Як результат, виявлено достатньо високу ступінь збіжності роботи протоколів DTN з іншими протоколами і різними середовищами передачі. Показано перспективність і актуальність даних мереж у майбутньому, розглянуті не повністю досліджені питання галузі.

В подальшому планується проаналізувати стан питання моделювання мереж DTN.

Список літератури

1. Delay-Tolerant Networking Architecture [Text] / V. Cerf, S. Burleigh, A. Hooke, L. Torgerson, R. Durst, K. Scott // Request for Comments. –2007. – № 4838. – 35 p.
2. InterPlanetary Networking Special Interest Group (IPNSIG) [Електронний ресурс] : [Веб-сайт]. – Електронні дані. – IPNSIG, 2015. – Режим доступу: www.ipnsig.org (дата звернення 05.06.2015) – Назва з екрана.
3. Wood Lloyd, Holliday Peter, Floreani Daniel and M. Wesley. Eddy, Sharing the dream // Workshop on the Emergence of Delay-/Disruption-Tolerant Networks (E-DTN), part of the International Conference on Ultra Modern Telecommunication (ICUMT).– St.

Petersburg: Russia, 14 October, 2009. – P. 1–4

4. Лукашенко, В. В. Сравнительный анализ и оптимизация протоколов для сетей с низкой чувствительностью к задержкам [Текст] / В. В. Лукашенко // Радиоэлектронні і комп'ютерні системи. – 2014, № 6 (70). - С. 145 - 149.

5. Special issue on DTN // Journal of Communications. – 2010. – V. 5. – № 2. – P. 106–130.6. Bundle Protocol Specification [Text] / K. Scott, S. Burleigh // Request for Comments. –2007. – № 5050. –50 p.

7. Licklider Transmission Protocol - Security Extensions [Text] / S. Farrell, M. Ramadas, S. Burleigh // Request for Comments. –2008. – № 5327. –11 p.

8. Bundle Security Protocol Specification [Text] / S. Symington, S. Farrell, H. Weiss, P. Lovell // Request for Comments. –2011. – № 6257. –60 p

9. Delay-Tolerant Networking TCP Convergence-Layer Protocol [Text] / M. Demmer, J. Ott, S. Perreault // Request for Comments. –2014. – № 7242. –22 p.

10. Казаков. М.Ф. Построение самоорганизующейся сети мобильных устройств / М.Ф. Казаков // Молодежь и наука: сборник материалов X Юбилейной Всероссийской научно-техн. конф. студентов, аспирантов и молодых ученых с международным участием. посвященной 80-летию образования Красноярского края . - Красноярск; Сиб. федер. ун-т. 2014.-С.13-17.

11. Tanenbaum, A. S. Computer Networks, 5th Ed. [Text] / Andrew S. Tanenbaum, David J. Wetherall. – Prentice Hall, Cloth, 2011. – 960 p

12. S. Jain, K. Fall, R. Patra, "Routing in a Delay Tolerant Network", Proceedings SIGCOMM, Aug/Sep 2004.

13. Networking for Communications Challenged Communities (N4C) [Електронний ресурс] : [Веб-сайт]. – Електронні дані. – The N4C Project, 2015. – Режим доступу: wiki.n4c.eu(дата звернення 07.06.2015) – Назва з екрана.

Статтю подано до редакції 28.08.2015