УДК 044.7(045)

Марченко В.В.

ВИЯВЛЕННЯ ПРОБЛЕМНИХ ДІЛЯНОК МЕРЕЖІ ДЛЯ ПРОВОДОВИХ І КОАКСІАЛЬНИХ КАНАЛІВ

Національний авіаційний університет

Запропоновано два механізми для віддаленої діагностики локальних мереж. Проаналізовано можливості застосування запропонованих алгоритмів віддаленої діагностики проводових або коаксіальних каналів. Отримано математичні співвідношення, що дозволяють виявити проблемні ділянки локальної мережі: несправні мережні пристрої, ділянки, що містять джерела наведень і спотворень

Вступ

На сьогоднішній день сфера передавання інформації є досить ускладненою. Мережі окремих підприємств та мережі зв'язку спеціального призначення об'єднуються у великі багатофункціональні мережі, здатні працювати з широким спектром завдань і надавати всі різновиди послуг зв'язку. Однак у таких мережах управління і контроль за використанням мережних ресурсів стають визначальними, оскільки індивідуальні програми можуть впливати на параметри функціонування системи в цілому. У цій ситуації технологія *QoS* призначена забезпечити у разі надходження трафіку "вищої" категорії задані значення параметрів незалежно від інтенсивності трафіку інших категорій [1].

Мета роботи – розробка алгоритмів для виявлення причин втрат пакетів в мережному каналі: втрати через переповнення буферів у мережних пристроях по шляху проходження або пошкодження пакетів під час транспортування.

Постановка задачі

Основних причин незадовільної роботи мережі може бути декілька: пошкодження кабельної системи, дефекти активного устаткування, перевантаженість мережних ресурсів. Часто одні дефекти мережі маскують інші. Для виявлення дійсних причин несправностей і збоїв, мережу потрібно комплексно продіагностувати. Завданням здійснених досліджень є розробити алгоритми віддаленої діагностики проводових та коаксіальних каналів.

Основна частина

Проблема забезпечення якості обслуговування є багатогранною, всебічно досліджуються питання про виявлення проблемних ділянок мережі, в яких відбуваються втрати пакетів, також вивчається механізм накопичення втрат пакетів. В теорії розроблено алгоритм віддаленої діагностики локальних мереж і випробувано його на практиці. Було також вивчено питання про вплив наведень і шумів на залежність ймовірності втрат пакетів від довжини пакету. Ці два дослідження дозволяють знаходити в мережі проблемні ділянки, які можуть сильно впливати на якість даних, які передаються через ці ділянки.

Алгоритм віддаленої діагностики проводових або коаксіальних каналів за допомогою аналізу втрат пакетів. Для будь-якої досить великої структурованої локальної мережі виникає проблема моніторингу її стану і виявлення перевантажених сегментів. Зазвичай це робиться із залученням можливостей протоколу *SNMP*, який дозволяє вимірювати завантаження в сегментах, якщо відповідне обладнання підтримує цей протокол. На жаль не будь-яке устаткування пристосоване для цього, і навіть *SNMP* керовані пристрої не завжди вміють реєструвати втрати пакетів у своїх внутрішніх буферах. Окрім того, високе завантаження ще не привід для занепокоєння, якщо всі дані, що пересилаються, успішно доставляються

адресатові. Отже було розроблено алгоритм, який дозволяє за допомогою однієї робочої станції, в реальному масштабі часу, цілодобово оцінювати роботу віддалених мережних сегментів. Як параметр, який характеризує якість роботи сегмента, використовується відсоток пакетів, загублених у сегменті. Підвищення ймовірності втрат пакетів особливо сильно впливає на ефективність роботи протоколу *TCP*. Проблемні сегменти виникають в області за перевантаженими мережними приладами. Якщо усереднене значення ймовірності втрати пакета уздовж маршруту перевищує деякий поріг (наприклад, 1%), слід розглянути можливість вибору іншого маршруту передавання даних.

На рис. 1 наведено схему, що пояснює запропонований алгоритм вимірювань.

N1, N2, ..., Nn – активні мережні пристрої, тобто такі прилади, де відбувається буферизація пакетів і можлива їх втрата.

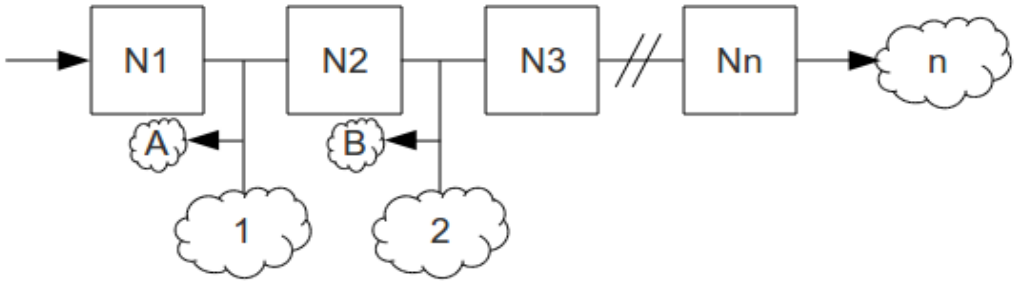

Рис. 1 Схема вимірювань

A, B, – це підмножина машин із мережних сегментів 1, 2 ,..., *n*, чиї мережні інтерфейси не дуже завантажені (наприклад, слабо завантажені робочі станції).

Тестова ЕОМ знаходиться в сегменті, підключеному до мережного пристрою *N1*. На ЕОМ встановлена програма, яка послідовно посилає *ICMP* запити до підмножини *A, B, ...* машин із сегментів *N1, N2, ..., Nn.* Та ж тестова ЕОМ обробляє *ICMP* відгуки, які прийшли із сегментів. *ICMP* відгуки мають ту ж довжину, що і *ICMP* запити. Вважається, що ймовірність втрати в проміжному пристрої для запиту і відгуку під час експерименту не змінюється й має однакове значення. Втрати в основному відбуваються через переповнення буферів в активних мережних пристроях.

Якщо на вхід каналу в *N1* надійшло S пакетів, спрямованих в субмережу *n* то з *N1* в *N2* надійде *S(1-α1)*, де *α1* - імовірність втрати пакету в активному пристрої *N1*, відповідно (*1-α1*) - доповнення події. За аналогією отримаємо вираз для кількості пакетів, що дійшли до сегмента *n* і повернулися до відправника - тестової ЕОМ:

$$R=S(1-\alpha 1)2(1-\alpha 2)2...(1-\alpha n-1)2(1-\alpha), \quad (1)$$

де αi - відсоток загублених пакетів у віддаленому сегменті *i, R* - кількість пакетів, які повернулися до відправника.

Друга степінь у множниках (*1-αi*) виникає через те, що пакети можуть губитися в мережних пристроях як по дорозі туди, так і назад. Під час відправки відгуку з машини сегменту n втрата неможлива, з цієї причини співмножник (*1-α*) має першу ступінь. На практиці вимірюємо величини *(1-α1)2, (1-α2)2* ,.... Пояснимо суть методу на прикладі фрагмента мережі, що наведено на рис. 2.

Кожен мережний пристрій на шляху *U1-U2-U3* має певний обсяг буфера *Bi* і завантаження (*Ii*). З цієї причини у нього є певна ймовірність втрат *x(Bi,Ii)*, що залежить від завантаження *I=I(t)* (*i* - номер мережевого пристрою). Зондування проводилося з допомогою пакетів *ICMP*, але для таких цілей можна використовувати також *TCP* або *UDP*.

Нехай *x1* - ймовірність втрати пакету на рівні *U1 (у CISCO 2948), x2* -

ймовірність втрати пакета на рівні *U2, x3* - ймовірність втрати пакету на рівні *U3*. Позначимо ймовірності втрат в мережних пристроях шарів 1, 2 і 3 як: *x1=x(B1,I1), x2=x(B2,I2), x3=(B3,I3)*.

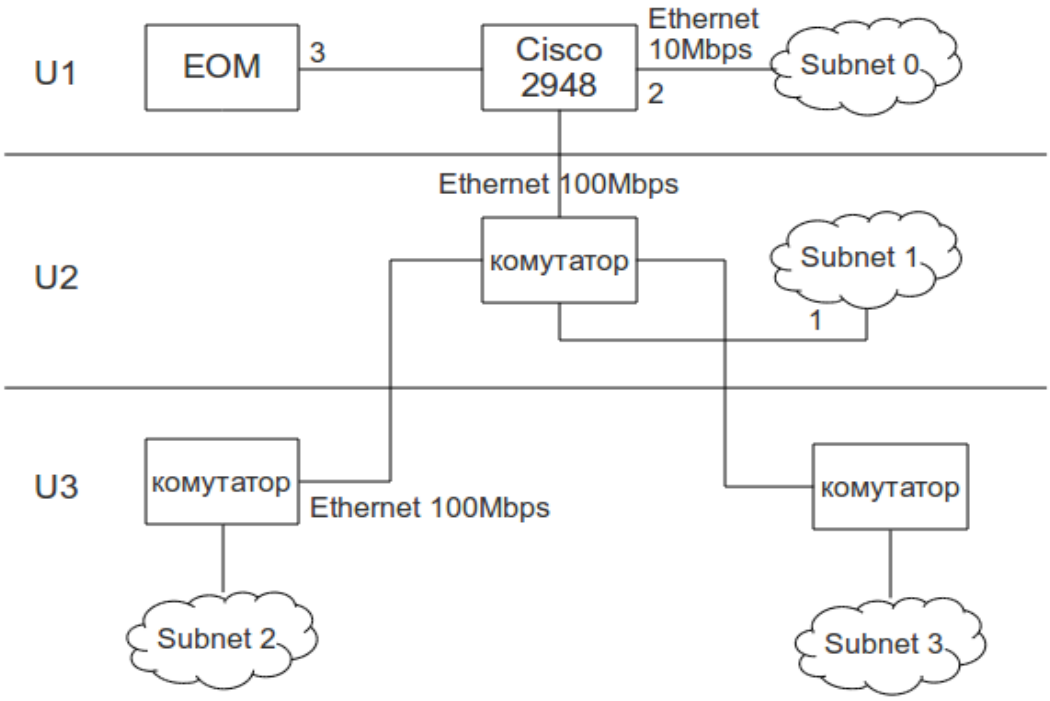

Рис. 2 Топологія тестової мережі

Робоча станція, що досліджується, знаходиться на рівні *U1* і з її допомогою вимірюються втрати в нижчих шарах. Зондуючи subnet0, визначимо усереднену ймовірність втрат пакетів на рівні 1 *(U1(t)=x1(t))*. В даному випадку розглядаємо незалежні події, а отже ймовірність одночасного настання двох незалежних подій дорівнює добутку ймовірностей цих подій [3]. Отже усереднена ймовірність втрат для сукупності ЕОМ на рівні *U2* (*subnet1*) дорівнює (2).

$$U2(t) = x1x2. \quad (2)$$

Знаючи *U1(t) і U2(t),* обчислюємо *x2=U2(t)/U1(t)*. Аналогічно визначаємо усереднену ймовірність втрат для сукупності машин на рівні *U3* (3).

$$U3(t) = x1x2x3. \quad (3)$$

Вимірюючи відсоток втрат для сукупності машин, що підключені до сегментів, які нас цікавлять, можна послідовно обчислити *x(B, I)* для кожної ланки цього шляху.

З бази даних ми беремо інформацію про приналежність тієї чи іншої IP-адреси ЕОМ до сегменту, який нас цікавить, і виконуємо зондування всіх машин субмережі. Кожна ЕОМ зондується послідовно серіями по три пакети. Якщо всі три пакета не дали відгуку, машина вважається виключеною, і ці дані не враховуються під час оцінки ймовірності втрати пакета. Такий підхід веде до певного заниження ймовірності втрат. Зате ми не завищуємо ймовірність втрат за рахунок відключених в даний момент ЕОМ.

Розглянутий алгоритм дозволяє віддалено виміряти ймовірність втрати пакетів для мережного сегмента, якщо відомий список *IP*-адрес цього сегмента і в кожному з мережних пристроїв по шляху є інтерфейс, де можна оцінити втрати в цьому конкретному мережному пристрої. Така ситуація звичайно легко

реалізується всередині локальної мережі, а також в опорних мережах сервіс провайдерів.

Використання залежності ймовірності втрати пакета від його довжини, як засіб діагностики транспортного каналу. Використовуючи канал з високою пропускною здатністю можна практично виключити буферизацію пакетів, яка є головною причиною більшості розбіжностей щодо якості обслуговування (*QoS*) (наприклад *VoIP*). Однак велика пропускна здатність досить дорога і не гарантує розв'язання всіх проблем, що можуть виникнути навіть у самих надійних *IP*-мережах. Проблеми будуть з'являтися та їх необхідно буде виявити і виправити. Тому важливо проводити превентивний контроль якості кожного з'єднання, що виконується в мережі, щоб негайно виявити і вирішити проблеми з якістю. У разі використання протоколу *TCP* втрати пакетів сповільнюють швидкість обміну даними, відбувається повторне передавання втрачених пакетів. Запропонований метод дозволяє визначати причини втрат пакетів.

Виявлення причини втрат пакетів в транспортному мережному каналі є корисним допоміжним засобом для пошуку ділянок мережі, які погано працюють. Причинами втрати можуть бути переповнення буферів у мережних пристроях на шляху проходження та пошкодження пакетів під час їх транспортування.

Якщо втрати пов'язані з пошкодженням пакетів під час транспортування, то залежність ймовірності втрат PL від довжини L пакету повинна характеризуватися залежністю

$$PL=(1-(1-p)L), \qquad (4)$$

де p – ймовірність пошкодження одного біта (*BER - Bit Error Rate*). З урахуванням того, що BER знаходиться в діапазоні 10-3- 10-10, а L>512 біт,

$$PL=(1-(1-L*p+0,5*p2L(L-1)+...)). \qquad (5)$$

Таким чином, можна очікувати квадратичну залежність ймовірності втрат від довжини пакета для малих *L*. Цю обставину можна використовувати для аналізу властивостей каналів. Вимірюючи залежність ймовірності втрат від довжини пакету, і апроксимуючи її методом найменших квадратів, можна ідентифікувати причини втрат.

Проведено дослідження втрат пакетів для кількох маршрутів. Для каналу Київ (вул. Леонтовича) – Москва (М-9) були проведені вимірювання ймовірності втрати для довжин пакетів 64, 128, 256, 512, 1024 і 1450 байт. Для кожної із довжин було надіслано по 2000 *ICMP*-пакетів. Результати вимірювань наведено на рис.3 і рис.4.

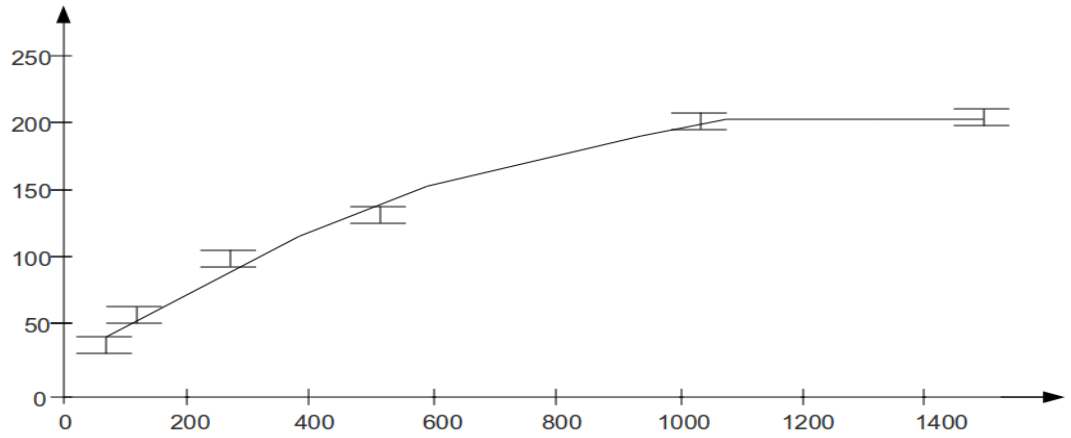

Рис. 3 Залежність числа втрачених пакетів (з 2000 надісланих пакетів) від довжини пакета для маршруту Київ - Москва. По вертикалі відкладено число втрачених пакетів, по горизонтальній осі відкладена довжина пакетів у байтах

У загальному вигляді має місце твердження (7).

$$Cpath=PL+F(L), \quad (7)$$

де *Cpath* повна ймовірність втрати пакета на всьому маршруті, *L* – число біт у пакеті, *F(L)* – функція відображає факт того, що ймовірність втрати пакета уздовж шляху проходження залежить від його довжини. *F(L)* – для різних мережних маршрутів буде різна, тому її значення оцінюється експериментально.

Апроксимація поліномом другої ступені за методом найменших квадратів дає таку залежність імовірності втрати пакета від його довжини.

$$Cpath =(14.33\pm6)+(0.298\pm0.04)L-(0.00012\pm3*10\text{-}5)L2. \quad (8)$$

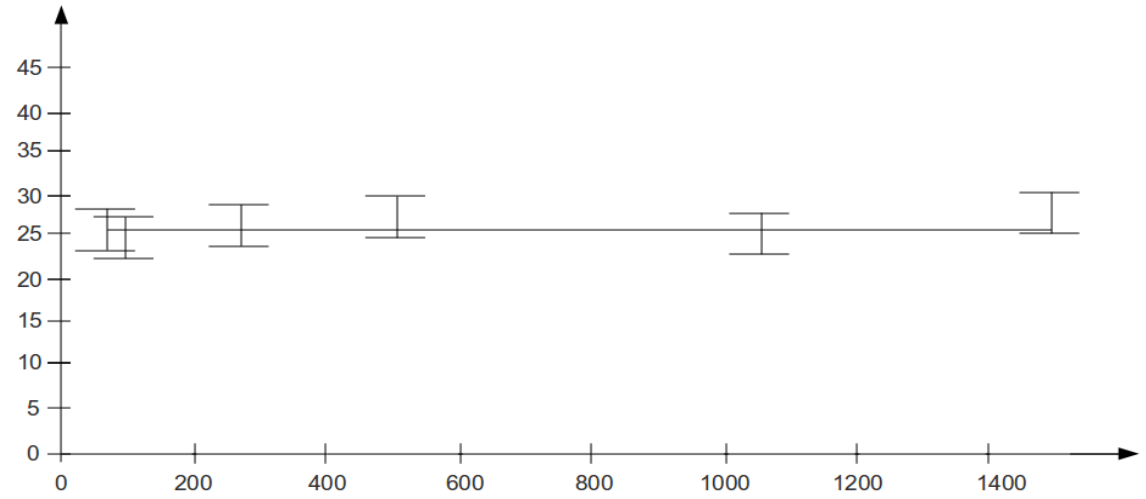

Рис. 4 Залежність числа втрачених пакетів (з 2000 відправлених пакетів) від довжини пакета для маршруту Київ (вул. Леонтовича) - Франкфурт (*decix*). По вертикалі відкладено число втрачених пакетів, по горизонтальній – довжину пакетів у байтах

$$Cpath =(25.56\pm4.42)+(0.00167\pm0.01)L-(9.46*10\text{-}7\pm1.23*10\text{-}5)L2. \quad (9)$$

Порівняння результатів показує, що в першому випадку (рис. 3) помітний вплив на втрати надає пошкодження пакетів під час проходження по маршруту. У другому випадку (рис. 4) імовірність втрати визначається переповненням буфера, ємність якого задається в сегментах.

Висновки

Звідси можна зробити висновок, що дослідження залежності ймовірності втрати від довжини пакету можна вважати корисним діагностичним засобом для дослідження властивостей каналів і виявлення втрат пакетів, що пов'язані зі спотвореннями переданих кадрів.

Ця методика дозволяє виявити ділянки мережі або каналу, що містять джерела наведень і спотворень. Корисним може бути порівняння залежностей ймовірності втрати пакета від його довжини, отриманих для одного і того ж каналу в різний час.

Список літератури

1. *Srinivas Vegesna*. "IP Quality of Service", Cisco Press 2001.

2. *А.А.Гончаров, Ю.А.Семенов.* «Выявление узких мест и неисправного сетевого оборудования с помощью анализа потерь пакетов.» XLV Научная конференция Московского Физико-технического института, 29-30 ноября 2002 года.

3. *Боровков А.А.* Теория вероятностей: Учеб. пособие для вузов. Москва: Наука 1986. – 432 с.

Подано до редакції 17.12.2010