УДК 004.7:519.2

**Торошанко Я. І., Хобта Б. М., Хобта П. М.** Державний університет телекомунікацій

# ЗАСОБИ УПРАВЛІННЯ ПЕРЕВАНТАЖЕННЯМИ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

*В роботі досліджені особливості, причини виникнення і основні шляхи запобігання перевантаження. Показана можливість запобігання перевантаження на основі способу розділення вхідного потоку на окремі вхідні черги, що надає можливість більш гнучко регулювати вхідний трафік вузла в умовах надзвичайних ситуацій. Показана також можливість використання методів і кількісних характеристик чутливості для визначення стану мережі.*

***Ключові слова:*** *комп'ютерна мережа, функції чутливості, маршрутизація, перевантаження, пропускна здатність*

**Вступ. Постановка задачі.** Ефективність використання мережі в значній мірі визначається якістю управління в умовах перевантаження. Коли в мережу надходить надто великий обсяг даних, може виникнути перевантаження, і робочі характеристики мережі погіршуються. При надмірних завантаженнях пропускна здатність (продуктивність) мережі може стати нульовою. Така ситуація може призвести до колапсу мережі.

Сьогодні існує велика кількість алгоритмів боротьби з перевантаженнями даних алгоритмів, які задовольняють ті чи інші потреби користувачів.

В роботі [1] представлена класифікація систем боротьби з перевантаженнями RED, які використовуються в протоколі TCP (Transmission Control Protocol) мережі інтернет. На основі даної роботи була запропонована розгорнута класифікація, яка доповнена іншими реалізаціями алгоритмів боротьби з перевантаженнями, які використовуються на сьогоднішній день [2]. Описані характеристики алгоритмів, визначені переваги та недоліки їх застосування в певних умовах роботи мереж.

Досить поширеним для боротьби з перевантаженнями є алгоритм TCP Veno, який здатен ефективно працювати як в проводових мережах, так і в безпроводових. В роботах [3, 4] розглядається використання даного алгоритму при стандартних значеннях його параметрів.

Подальші дослідження показали можливість збільшення пропускної здатності мережі шляхом оптимізації параметрів алгоритму TCP Veno [5].

Причиною перевантаження може бути недостатній об'єм пам'яті для вхідних буферів або невелика швидкодія процесора маршрутизатора. Однак, слід зауважити, що значне збільшення об'єму пам'яті вхідних буферів може призвести до збільшення негативних наслідків, пов'язаних з перевантаженням [6]. Пояснення цього полягає в тому, що із зростанням об'єму буферної пам'яті збільшується кількість необроблених пакетів і час очікування їх обробки може перевищити допустимі норми тривалості тайм-ауту, при цьому з'являються повторно передані пакети, що призводить до подальшого зниження корисної пропускної здатності мережі. Іншими словами, перевантаження може бути причиною виникнення лавинного процесу: переповнення буфера призводить до втрати пакетів, які доведеться передавати повторно або навіть кілька разів. Таким чином, обчислювальний вузол маршрутизатора-відправника отримує надлишкове паразитне завантаження.

Причиною перевантаження може бути повільний процесор або "вузьке горло" – низька пропускна здатність окремої дільниці мережі. Просте підвищення швидкодії процесора або інтерфейсу не завжди усуває проблему – вузьке місце, як правило, переноситься в інший сегмент мережі.

**Способи боротьби з перевантаженнями.** Перевантаження мережі, як правило, носить тимчасовий характер і означає, що вхідне навантаження на даному проміжку часу перевищило можливості ресурсів даної частини системи. Рішення даної задачі може здійснюватись за двома напрямками: збільшення ресурсів системи і регулювання вхідного трафіку перевантаженої ділянки мережі [7-9].

Перший шлях залежить від конкретної реалізації та наявності додаткових ресурсів. Наприклад, у супутникових системах підвищення продуктивності (пропускної спроможності) може бути досягнуто за рахунок збільшення потужності передавача. В локальних підмережах можуть тимчасово використовуватись телефонні лінії з модемами між певними її точками. У випадку надзвичайних ситуацій може використовуватись резервне обладнання, запасні маршрутизатори тощо. Задача уникнення або зменшення рівня перевантаження може також вирішуватись на рівні підсистеми маршрутизації шляхом розподілу трафіку по декількох маршрутах замість постійного використання одного і того ж, нехай навіть оптимального шляху.

У випадку, коли немає можливості збільшувати пропускну спроможність або вона уже збільшена до межі, єдиний спосіб боротьби з перевантаженням полягає в зменшенні навантаження шляхом зниження рівня обслуговування деяких або всіх користувачів, включаючи відмову в їх обслуговуванні.

Одним з поширених методів боротьби з перевантаженнями є управління зі зворотним зв'язком. Механізм і завдання управління вирішується на транспортному рівні засобами протоколу TCP [7, 9, 10]. При виявленні перевантаження швидкість передачі знижується шляхом зменшення розміру ковзного вікна.

По суті, має місце управління з зворотним зв'язком, що запізнюється. При неправильному обрахуванні характеристик запізнювання система може втратити стійкість і перейти в незатухаючий коливальний режим, або коригування інтенсивності потоку буде здійснюватися занадто пізно [6, 10]. Компенсація затримки зворотного зв'язку може виконуватися методами передбачення, наприклад, з використанням моделі авторегресії і ковзного середнього (АРКС) або шляхом усереднення параметрів вікна. Другий варіант простіший, але, природно, забезпечує значно більш низьку якість сервісу.

Позитивного результату також можна досягти шляхом варіації значень тайм-аутів, зміною протоколів квитування і повторної передачі пакетів, зміною схеми буферизації.

Управління зі зворотним зв'язком широко використовується в архітектурі інтегрованих служб (Integrated Service Architecture – ISA) для підтримки служб з різними рівнями якості сервісу (Quality of Service – QoS) в Інтернеті і в приватних об'єднаних мережах [7, 8, 11].

Для систем без зворотного зв'язку вирішення проблеми вирівнювання швидкості передачі даних може бути вирішено за допомогою алгоритмів “дірявого відра” і “маркерного відра” [8, 12]. Алгоритм “дірявого відра”, являє собою механізм регулювання трафіку, коли частина потоку пакетів, що перевищує пропускну здатність мережі, просто відкидається або позначається як надлишкова або низько пріоритетна.

**Альтернативна маршрутизація.** Розглянемо один з випадків боротьби з перевантаженням способом альтернативної маршрутизації. В разі неможливості пропускання трафіку через перевантажений або пошкоджений з тих чи інших причин вузол потрібно знайти альтернативний шлях передачі пакетів.

Як приклад, розглянемо випадок системи обслуговування, коли до вузла надходять вхідні інформаційні потоки IS1, IS2 та IS3, які об’єднуються у спільну вхідну чергу IQ (рис. 1).

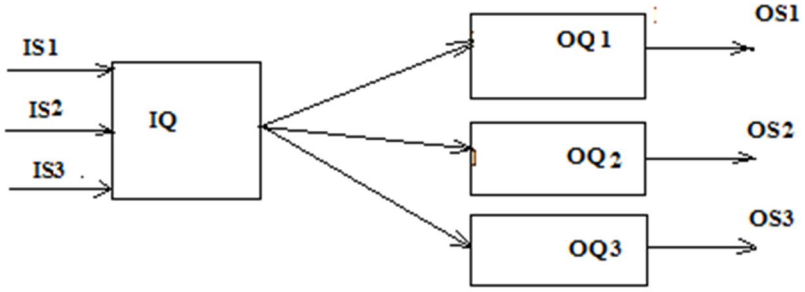


Рис. 1. Система обслуговування із спільною вхідною чергою

Із вхідної черги IQ згідно поточного алгоритму (таблиць) маршрутизації формуються вихідні черги OQ1, OQ2, OQ3 і відповідні їм вихідні потоки OS1, OS2, OS3.

На перші два потоки IS1 та IS2 поступає певна кількість пакетів даних, яка передається до вузлів призначення. В третьому потоці IS3 передається об'єм даних, де окрім даних джерела, яке зазвичай передає дані в цій мережі, також передаються дані, які передаються по альтернативному маршруту. Це створює додаткове навантаження і, як наслідок, спричиняє виникненню перевантаження вхідної черги IQ, а також тих чи інших вихідних черг. Одним із ефективних способів запобігання перевантаженню є тимчасове відключення потоків, які не пов’язані із надзвичайною ситуацією. Таким чином, планується зменшити навантаження на вході вузла. Враховуючи, що потоки взаємопов'язані, відключення одного потоку призведе до відключення всіх потоків. Як наслідок, через цей вузол не буде передано жоден з пакетів даних (рис. 2), що не вирішує проблему перевантаження без втрати пакетів і погіршення якості обслуговування, що тільки погіршує поточний стан мережі.

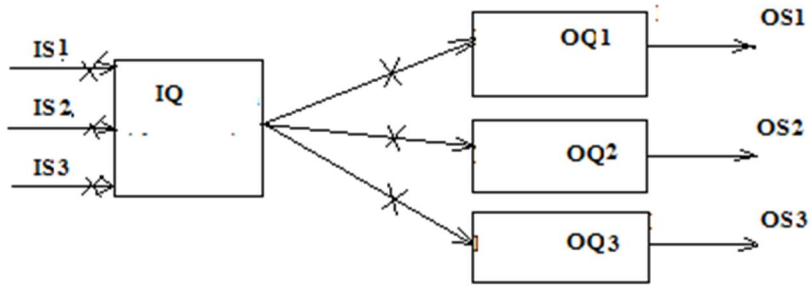


Рис. 2. Система з тимчасовим відключенням потоків спільної вхідної черги

Рішенням такої задачі може бути розділення спільної вхідної черги IQ на три незалежні черги IQ1, IQ2, IQ3 відповідно до вхідних потоків IS1, IS2, IS3 (рис. 3). Зауважимо, що можливі і змішані системи (при більшому числі вхідних потоків), коли певні групи вхідних потоків об’єднуються у спільні вхідні черги, кожна з яких розглядається незалежно одна від одної.

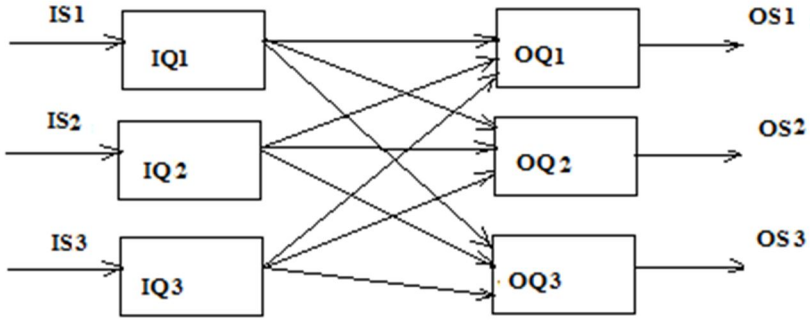


Рис. 3. Система з розділенням потоків вхідної черги

Застосувавши представлений вище метод, ми можемо відключити потоки IQ1 та IQ2 (рис. 4).

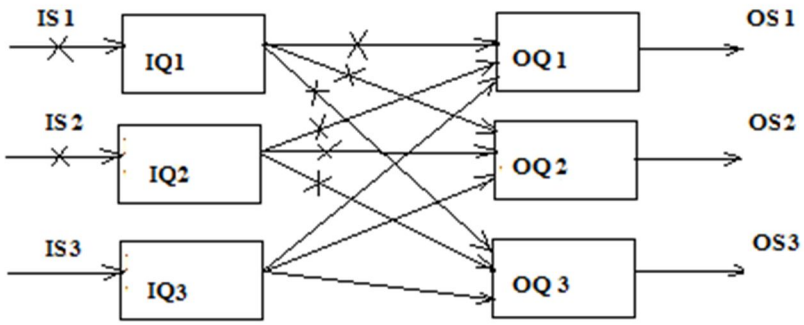


Рис. 4. Система з блокуванням потоків вхідної черги

Таким чином, зменшивши таким чином інформаційне навантаження на вузол не блокуючи потік IQ3, пов'язаний із надзвичайною ситуацією. Після обробки інформації перевантаженої черги відключені потоки розблоковуються і вузол переходить у штатний режим функціонування в. мережі. Отже, зазначений спосіб є ефективним для другого випадку. Переваги цього способу є ефективність і простота реалізації, відсутність додаткових затрат на обладнання, універсальність (даний спосіб можна пристосувати і для вирішення інших задач).

**Управління перевантаженням.** В комп'ютерних мережах без резервування ресурсів, управління повинно бути реакційним. Схема реакційного управління перевантаженням може бути впроваджена в двох місцях: – в комутаторах, де виникає перевантаження; – в джерелах, в яких контролюється надходження пакетів в мережу. Як правило, комутатор використовує деякий набір даних (наприклад, переповнення буферів) для визначення виникнення перевантаження, і непрямим чином чи недвозначно передає цю проблему джерелам, які зменшують їхній вхідний трафік. Існують декілька альтернатив виявлення/уникнення перевантаження, основними з яких є [7, 8, 13, 14]:

– контроль заповненості та середнього часу зайнятості вхідних буферів, найбільш прийнятний при розділених вхідних чергах (рис. 3);

– контроль використання вихідних ліній (вихідних черг OQ, рис. 1, 3): встановлено, що перевантаження виникає, коли використання мережі переходить поріг чутливості приблизно 90%, і цей показник може бути використаний як сигнал попередження перевантаження.

– аналіз кругових затримок пакетів: зростання цих затримок свідчить про збільшення розміру черги і можливості перевантаження;

– постійне відстежування стану мережі, використовуючи певну схему дослідження.

Сигналізація і повідомлення про перевантаження від перевантаженого вузла на джерело може бути явним чи неявним. Коли повідомлення являється явним, комутатор посилає інформацію в заголовках пакета чи у відповідних керуючих пакетах (службові управляючі команди подавлення джерела, стримування, пакети оновлення стану, повідомленнях про управління швидкістю тощо). Сигналізація явних перевантажень викликає додаткове навантаження в мережі, так як мережа потребує передачі більшої кількості пакетів, ніж зазвичай. Це може призвести до втрати продуктивності, якщо часові витрати на сигналізацію не контролюються належним чином.

У випадку неявної сигналізації виявлення перевантаженого вузла здійснюється джерелом, – як правило за признаками перевищення заданого часу очікування (тайм-ауту) підтвердження виданих в мережу пакетів.

**Висновки**

В роботі досліджені особливості, причини виникнення і основні шляхи запобігання перевантаження. Показана можливість запобігання перевантаження на основі способу розділення вхідного потоку на окремі вхідні черги, що надає можливість більш гнучко регулювати вхідний трафік вузла в умовах надзвичайних ситуацій. Показана також можливість використання методів і кількісних характеристик чутливості для визначення стану мережі.

**Список використаної літератури**

1. Королькова А. В. К вопросу о классификации алгоритмов RED / А. В. Королькова, Д. С. Кулябов, А. И. Черноиванов // Вестник Российского университета дружбы народов. – 2009. – №3. – С. 34-46.

2. Максимов В. В. Класифікація алгоритмів боротьби з перевантаженнями / В. В. Максимов, С. О. Чмихун // Наукові записки Українського науково-дослідного інституту зв'язку. – 2014. – № 5(33). – С. 73-79.

3. Галкин А. М. Пакет моделирования NS-2 / А. М. Галкин, Е. А. Кучерявый, Д. А. Молчанов ; учебное пособие. – Санкт-Петербург, СПбГТ, 2007.

4. Сиропятов О. А. Проблема моделювання трафіку у мережах доступу до недовірених систем / О. А. Сиропятов, Н. Ф. Казакова // Інформаційна безпека. – 2013. – № 1(9). – С. 185-189.

5. Максимов В. В. Дослідження алгоритму боротьби з перевантаженнями TCP VENO / В. В. Максимов, С. О. Чмихун // Телекомунікаційні та інформаційні технології. – 2015. – №4. – С. 30-36.

6. Виноградов Н.А., Дрововозов В.И., Лесная Н.Н., Зембицкая А.С. Анализ нагрузки на сети передачи данных в системах критичного применения / Н. А. Виноградов, В. И. Дрововозов, Н. Н. Лесная, А. С. Зембицкая // Зв'язок. – 2006. – № 1 (61). – С. 9-12.

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

8. Stallings W. Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud / W. Stallings. – Pearson Education, Inc., Old Tappan, New Jersey, 2016. – 544 p.

9. Виноградов Н. А. Сеть передачи данных как объект управления / Н. А. Виноградов // IV Міжнародна науково-технічної конференції «Комп'ютерні системи та мережні технології (CSNT-2012)», м. Київ, 13-15 червня 2012 р., НАУ. – 34 с.

10. Vinogradov N. A. Comparative analysis of the functionals of optimal control corporate computer network / Nick A. Vinogradov, Alina S. Savchenko. – Journal of Qafqaz University (Mathematics and Computer Science). – 2013, Vol. 1, Nr. 2. – PP. 156-167.

11. Kharlay L. Adaptive control of traffic flows and congestions in computer corporate networks / Lyudmyla Kharlay, Andriy Skrypnichenko, Chang Shu, Yaroslav Toroshanko // East European Scientific Journal. – 2016. – №9. – PP. 67-72.

12. Козелкова Е. С. Управление потоками данных в цифровых телекоммуникационных сетях с разнородным трафиком / Е. С. Козелкова, Я. И. Торошанко, Л. А. Харлай // Вісник Національного університету «Львівська політехніка». Серія «Радіоелектроніка та телекомунікації». – 2016. – №819.

13. Arulambalam A. Allocating Fair Rates for Available Bit Rate Service in ATM Networks / A. Arulambalam, X. Chen, N. Ansari // IEEE Comun. Mag., Nov. 1996. – PP. 92-100.

14. Chen T. M. The Available Bit Rate Service for Data in ATM Networks / T. M. Chen , S. S. Liu, V. K. Samalam // IEEE Commun. Mag. – May 1996. – PP. 56-71.

***Автори статті***

**Торошанко Ярослав Іванович –** кандидат технічних наук, професор кафедри комп'ютерної інженерії, Державний університет телекомунікацій, м. Київ. Тел. +380 (50) 555 51 14. E-mail: toroshanko@ukr.net.

**Хобта Богдан Михайлович** – студент, кафедра комп'ютерної інженерії. Державний університет телекомунікацій, м. Київ. Тел.: +380 (50) 066 76 41. E-mail: bios_level@ukr.net.

**Хобта Павло Михайлович** – студент, кафедра комп'ютерної інженерії. Державний університет телекомунікацій, м. Київ. Тел.: +380 (95) 891 60 73. E-mail: hpavel2017@ukr.net.

***Authors of the article***

**Toroshanko Yaroslav Ivanovych –** candidate of sciences (technical), professor of computer sciences department, State University of Telecommunications, Kyiv. Tel. +380 (50) 555 51 14. E-mail: toroshanko@ukr.net.

**Khobta Bohdan Mykhailovych** – student, computer sciences department. State University of Telecommunications, Kyiv. Tel. +380 (50) 066 76 41. E-mail: bios_level@ukr.net.

**Khobta Pavlo Mykhailovych** – student, computer sciences department. State University of Telecommunications, Kyiv. Tel. +380 (95) 891 60 73. E-mail: hpavel2017@ukr.net.

Дата надходження
в редакцію: 17.09.2016 р.

Рецензент:
доктор технічних наук, професор К. С. Козелкова
Державний університет телекомунікацій