Wydanie V

SIECI KOMPUTEROWE

TANENBAUM | WETHERALL

Najpopularniejsze na świecie wprowadzenie do sieci komputerowych — w pełni zaktualizowane i przygotowane na technologie przyszłości

Tytuł oryginału: Computer Networks (5th Edition)

Tłumaczenie: Przemysław Szeremiota na podstawie „Sieci komputerowe” w tłumaczeniu Andrzej Grażyńskiego i Adama Jarczyka

ISBN: 978-83-246-3079-0

Wydawnictwo HELION
ul. Kościuszki 1c, 44-100 GLIWICE
tel. 32 231 22 19, 32 230 98 63
e-mail: helion@helion.pl
WWW: http://helion.pl (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
http://helion.pl/user/opinie?gimpbi
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

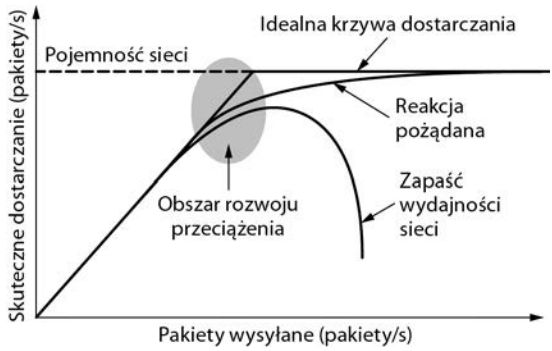
Printed in Poland.

SPIS TREŚCI

5.3. ALGORYTMY KONTROLI PRZECIĄŻEŃ

Nadmierna liczba pakietów obecna w sieci albo w jej części doprowadza do opóźnienia rozprowadzania pakietów i w efekcie do utraty wydajności. Sytuacja taka nosi nazwę **przeciążenia**. Odpowiedzialność za radzenie sobie z przeciążeniami ruchu jest podzielona pomiędzy warstwę sieciową i transportową. Skoro do przeciążeń dochodzi w sieci, doświadcza ich przede wszystkim warstwa sieciowa i to ona ostatecznie musi zaradzić powstałemu problemowi nadmiaru pakietów. Z drugiej strony, obciążenie wynika z natężenia ruchu przenoszonego przez warstwę transportową. Dlatego dla skutecznego unikania i eliminowania przeciążeń konieczna jest współpraca warstwy sieciowej i transportowej. W tym rozdziale przyjrzymy się aspektom przeciążeń w warstwie sieciowej. Temat przeciążeń dokończymy, omawiając aspekty warstwy transportowej w rozdziale 6.

Rysunek 5.19 ilustruje rozwój przeciążenia sieciowego. Kiedy liczba pakietów wysyłanych do sieci przez stację mieści się w zakresie zdolności przenoszenia sieci, liczba pakietów dostarczonych jest wprost proporcjonalna do liczby pakietów wysłanych. Kiedy host wysyła dwukrotnie więcej pakietów, odbiorca też dostanie ich dwa razy więcej.



Rysunek 5.19. Przy nadmiernym ruchu efektywność sieci zaczyna maleć

Ale kiedy liczba ta będzie zbliżać się do granicznej przepustowości sieci, serie pakietów mogą momentami doprowadzać do wysycenia buforów w routerach rozprowadzających pakiety, co z kolei oznacza utratę niektórych pakietów. Utracone pakiety zużywały pewną część przepustowości, więc liczba pakietów dostarczonych zaczyna być mniejsza od liczby pakietów wysłanych — krzywa dostarczania zaczyna odbiegać od prostej. Mówimy wtedy o przeciążeniu sieci.

Jeśli sieć jest słabo zaprojektowana, może w niej dojść do zapaści, gdy liczba wysyłanych pakietów przekroczy przepustowość sieci. Może to być wynikiem choćby tego, że opóźnienie rozprowadzania pakietów może je unieważniać w miejscu przeznaczenia. Na przykład we wczesnej fazie rozwoju Internetu czas, jaki pakiet spędzał w oczekiwaniu na rozprowadzenie na powolnym, 56-kilobitowym łączu, mógł przekraczać czas, po którym nadawca decyduje się na ponowne wysłanie pakietu z powodu braku potwierdzenia odebrania. Dochodzi wtedy do powielania pakietów wysyłanych do sieci, co niewątpliwie zwiększa przeciążenie i zmniejsza jej wydajność. Na osi *y* na rysunku 5.19 zaznaczono więc wartość skutecznego dostarczania, to znaczy liczbę przydatnych pakietów przenoszonych przez sieć.

Pożądana jest sieć, w której do przeciążeń nie dochodzi, a już na pewno nie dochodzi do zapaści w wyniku przeciążenia. Niestety, przeciążenia nie zawsze da się uniknąć. Jeśli nagle strumienie pakietów zaczną przychodzić na trzech lub czterech liniach wejściowych i wszystkie będą wymagały tej samej linii wyjściowej, powstanie kolejka. Jeżeli w pamięci braknie miejsca na wszystkie te dane, pakiety zaczną się gubić. Rozbudowa pamięci może pomóc do pewnego punktu, lecz Nagle (1987) uzmysłowił nam, że gdyby routery miały nieskończoną pojemność pamięci, przeciążenia stałyby się większe, a nie mniejsze, ponieważ do czasu dotarcia do początku kolejki pakiety traciłyby ważność (raz za razem) i źródło wysyłałoby duplikaty, co nie poprawia sytuacji, tylko ją pogarsza — prowadzi bowiem wprost do zapaści.

Źródłem przeciążeń sieci są również łącza o niskiej przepustowości albo routery, które przetwarzają pakiety wolniej, niż one napływają. W takim przypadku sytuację można poprawić poprzez kierowanie części ruchu poza wąskie gardła sieci; ostatecznie

jednak przy stałym wzroście ruchu przeciążenie musi objąć wszystkie regiony sieci. W takiej sytuacji nie ma wyjścia: trzeba albo okroić ruch, albo zbudować szybszą sieć.

Warto tu wyjaśnić różnicę pomiędzy kontrolą przeciążeń i sterowaniem przepływem, ponieważ ich związek jest bardzo subtelny. Kontrola przeciążeń ma gwarantować, że sieć będzie w stanie przenieść cały wprowadzany do niej ruch. Jest to problem globalny, obejmujący zachowanie wszystkich hostów i wszystkich routerów. Z kolei sterowanie przepływem odnosi się do ruchu pomiędzy konkretnymi nadawcami i odbiorcami. Jego zadaniem jest gwarantowanie, że szybki nadajnik nie będzie stale wysyłał danych szybciej, niż odbiornik będzie mógł je przyjmować.

Aby zrozumieć różnicę pomiędzy tymi dwoma mechanizmami, wyobraźmy sobie sieć złożoną ze 100-gigabitowych łączy optycznych, w której superkomputer usiłuje wtłoczyć duży plik do komputera osobistego, którego interfejs działa z prędkością zaledwie 1 Gb/s. Wprawdzie przeciążenie nie wystąpi (sieć nie ma kłopotów), lecz potrzebne będzie sterowanie przepływem, aby zmuszać superkomputer do częstych postojów, dających komputerowi osobistemu szansę odetchnąć.

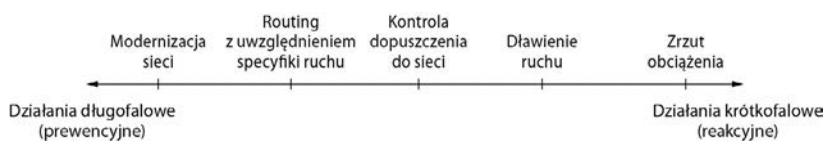
Drugą skrajnością może być na przykład sieć z buforowaniem mająca łącza 1 Mb/s i 1000 dużych komputerów, z których połowa usiłuje przesyłać pliki z szybkością 100 kb/s do drugiej połowy. Tutaj problem nie polega na przytłaczaniu odbiornika przez szybki nadajnik, lecz na przekroczeniu przez całkowity oferowany ruch możliwości sieci.

Powodem częstego mylenia sterowania przepływem i kontroli przeciążeń jest fakt, że najlepszym rozwiązaniem obu jest spowolnienie nadawców pakietów. Wobec tego host może otrzymać komunikat „zwolnij” albo dlatego, że z obciążeniem nie radzi sobie odbiornik, albo dlatego, że nie radzi sobie sieć. Wrócimy do tej kwestii w rozdziale 6.

Zaczniemy analizę kontroli przeciążeń od spojrzenia na podejścia, które stosuje się w różnych skalach czasowych. Potem zajmiemy się zapobieganiem przeciążeniom, a następnie sposobom postępowania, kiedy jednak się pojawią.

5.3.1. Metody kontroli przeciążeń

Obecność przeciążenia oznacza, że obciążenie sieci (czasowo) przekracza zasoby sieciowe (albo przynajmniej zasoby któregoś regionu sieci). Przychodzą wtedy na myśl dwa rozwiązania: zwiększenie zasobów albo zmniejszenie obciążenia. Na rysunku 5.20 widać, że rozwiązania te są zazwyczaj realizowane łącznie, ale w różnych horyzontach czasowych, aby z jednej strony reagować na obecne przeciążenia, a z drugiej unikać przyszłych.



Rysunek 5.20. Krótko- i długofalowe działania eliminujące przeciążenia

Najprostszym sposobem unikania przeciążenia jest zbudowanie sieci, która dokładnie odpowiada specyfice przenoszonego w niej ruchu. Jeśli na linii, którą idzie większość pakietów, znajduje się powolne łącze, przeciążenie sieci jest więcej niż prawdopodobne. Niekiedy w obliczu poważnego przeciążenia można zasilać sieć nowymi zasobami, na przykład włączając rezerwowe routery czy też dołączając łącza, które normalnie służą wyłącznie do zabezpieczenia redundancji (na wypadek fizycznych awarii łączy podstawowych). Można też na szybko nabywać przepustowość oferowaną na wolnym rynku przez innych operatorów. Zwykle te routery i łącza, które są najczęściej przeciążone, są modernizowane w najbliższym możliwym terminie. Odbywa się to już jednak w horyzoncie co najmniej miesięcy i wyłącznie po potwierdzeniu długofalowego trendu w ruchu sieciowym.

Aby możliwie dobrze wykorzystać dostępną pojemność sieci, routery powinny być przystosowane do wzorców obsługiwanego ruchu i do ich ewentualnych zmian w czasie (np. do zmian dobowego obciążenia poszczególnych łączy). Można na przykład na routerach odciągać ruch z najbardziej obciążonych tras poprzez tymczasową zmianę wag poszczególnych ścieżek. W niektórych stacjach radiowych i telewizyjnych stosuje się napowietrzną obserwację stanu dróg w mieście, umożliwiającą podawanie kierowcom informacji o korkach. Analogiczne obserwacje i dostosowania można prowadzić w sieciach komputerowych — mówimy wtedy o **routingu z uwzględnieniem warunków ruchu** (ang. *traffic-aware routing*). Pomocny bywa również rozdział ruchu pomiędzy alternatywne ścieżki dostarczania.

Niekiedy jednak zwiększenie (choćby tymczasowe) pojemności sieci jest niemożliwe; wtedy przeciążenie można zatrzymać wyłącznie poprzez zmniejszenie obciążenia ze strony nadawców pakietów. W sieciach z obwodami wirtualnymi odrzuca się wtedy nowe połączenia, bo doprowadziłyby do zapaści wydajności sieci. Takie działania noszą miano **sterowania dopuszczeniem do sieci** (ang. *admission control*).

Na niższym poziomie w obliczu przeciążenia sieć sama może dostarczać nadawcom pakietów wskazówki, aby ci zmniejszyli prędkość swoich transmisji. Można wtedy mówić o dławieniu ruchu ze strony nadawców albo o zrzucie obciążenia ze strony samej sieci.

Problemem jest tutaj samo wykrycie zbliżającego się przeciążenia oraz sposoby informowania nadawców o konieczności spowolnienia transmisji. Pierwszą kwestię rozwiązuje się mechanizmami monitorowania na routerach sieciowych, rejestrujących średnie opóźnienia kolejkowania pakietów, średnie obciążenie przetwarzaniem i stopień utraty pakietów. We wszystkich przypadkach rosnące wartości wskazują na rosnące przeciążenie.

Co do drugiego problemu konieczne jest uczestnictwo routerów w pętli zwrotnej informacji nadawców pakietów. Aby taka metoda działała poprawnie, zależności czasowe muszą być dokładnie regulowane. Gdyby po każdym dotarciu dwóch pakietów pod rząd router krzyczał: „Stop!”, a po każdym okresie bezczynności routera wynoszącym 20 μs krzyczał: „Dalej!”, system oscylowałby gwałtownie i nigdy się nie ustabilizował. Gdyby z drugiej strony czekał 30 minut na nabranie pewności przed powiedzeniem czegokol-

wiek, mechanizm kontroli przeciążeń reagowałby zbyt ślamazarnie, aby do czegokolwiek się nadawać. Dostarczanie na czas wskazówek co do dopuszczalnej prędkości transmisji nie jest wcale proste; do tego routery niefrasobliwie dostarczające takie powiadomienia same z siebie przyczyniają się do wzrostu obciążenia sieci. Ostatecznie kiedy wszystko inne zawiedzie, sieć jest zmuszona do odrzucania pakietów, których nie jest w stanie dostarczyć. Mówi się wtedy o **zrzucie obciążenia** (ang. *load shedding*). Tutaj dla zapobiegania przeciążeniom i eliminowania ich istotna jest wyważona polityka wyboru odrzucanych pakietów.

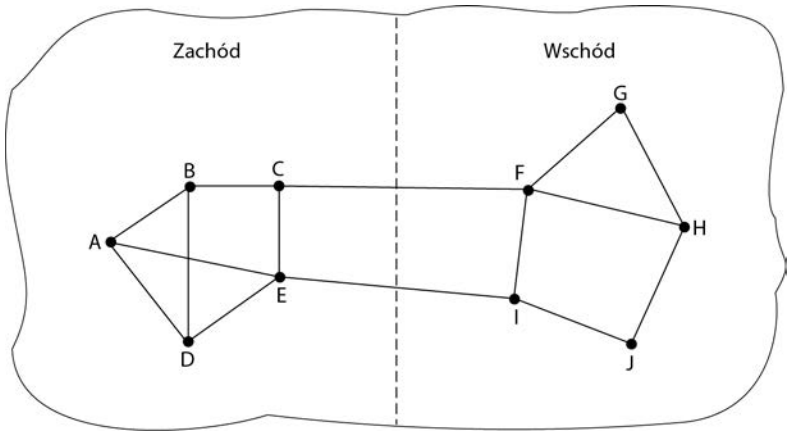
5.3.2. Routing z uwzględnieniem warunków ruchu

W pierwszej kolejności zajmiemy się routingiem z uwzględnieniem warunków ruchu. Metody routingu omawiane w podrozdziale 5.2 wykorzystywały stałe, predefiniowane wagi dla poszczególnych łączy. Adaptowały się do zmian w topologii sieci, ale nie do zmian w jej obciążeniu. Kiedy mówimy o wyznaczaniu tras z uwzględnieniem obciążenia poszczególnych fragmentów sieci, chcemy wyznaczać trasy tak, aby oddalać ruch od wąskich gardeł, które będą pierwszymi miejscami narażonymi na przeciążenia.

Najbardziej oczywistym sposobem na to jest zdefiniowanie wagi łącza jako funkcji (stałej) przepustowości łącza oraz opóźnienia propagacji sygnału plus (zmiennej) mierzonego obecnie obciążenia przetwarzania albo średniego opóźnienia kolejkowania pakietów. Podobne pod względem innych kosztów ścieżki są wtedy różnicowane za pomocą wydajności, a algorytm routingu powinien dobierać te, które mają mniejszą wartość funkcji wagi.

Routing z uwzględnieniem warunków ruchu był w takim wydaniu stosowany już we wczesnej sieci Internet (Khanna i Zinky, 1989), ale nie bez kłopotów — weźmy sieć z rysunku 5.21, podzieloną na dwie części: Wschód i Zachód, spięte dwoma łączami: *CF* i *EI*. Załóżmy, że większość ruchu pomiędzy wschodem i zachodem odbywa się za pośrednictwem łącza *CF*, w efekcie czego łącze to jest mocno obciążone i cechuje się dużymi opóźnieniami. Uwzględnienie opóźnienia kolejkowania w wadze używanej do wyznaczania najkrótszej ścieżki sprawi, że łącze *EI* zyska priorytet. Po zainstalowaniu nowych tabel routingu większość ruchu między wschodem i zachodem będzie się odbywać łączem *EI*, mocno je obciążając. W efekcie po następnej aktualizacji tablic routingu lepszym łączem okaże się ponownie *CF*. Ostatecznie dojdzie do oscylacji tabel routingu, co będzie destabilizowało routing i prowokowało liczne inne problemy.

Jeśli w wyznaczaniu najkrótszej trasy zignorujemy parametr obciążenia i uwzględnimy tylko opóźnienia propagacji pakietów, powyższy problem nie zaistnieje. Z kolei próby uwzględniania obciążenia, ale przy ograniczonym współczynniku owocują jedynie zmniejszeniem częstotliwości oscylacji routingu. Skuteczne rozwiązanie wymaga zastosowania jednej z dwóch technik. Pierwsza z nich to routing wielościeżkowy, dopuszczający obecność w tablicach routingu wielu tras do danego odbiorcy. W naszym przykładzie oznaczałoby to rozłożenie obciążenia pomiędzy oba łącza: Wschód – Zachód. Druga



Rysunek 5.21. Sieć, w której Zachód i Wschód są spięte dwoma łączami

technika to stopniowe przełączanie ruchu pomiędzy routerami, na tyle powolne, aby mogły one w międzyczasie aktualizować parametry łączy i ostatecznie osiągnąć stabilność tablic routingu, jak w metodzie Gallaghera (1977).

Z uwagi na powyższe trudności w protokołach routingu w Internecie unika się dostosowywania tras na podstawie obciążenia. Ewentualne dostosowania odbywają się za to poza protokołem routingu — zmieniane są więc jego dane wejściowe, a nie algorytm. Mówimy wtedy o **inżynierii ruchu**.

5.3.3. Kontrola dopuszczenia do sieci

W sieciach z obwodami wirtualnymi powszechnie stosowaną techniką unikania przeciążeń jest **kontrola dopuszczenia do sieci**. Pomysł jest prosty: nie wolno dopuszczać do tworzenia nowych obwodów wirtualnych, jeśli sieć nie będzie w stanie obsłużyć ruchu w tych obwodach. Próba zestawienia obwodu wirtualnego w takich warunkach powinna zostać zablokowana. To znacznie lepsze rozwiązanie niż dopuszczenie do sieci już obciążonej, a wkrótce przeciążonej. Analogicznie w systemie telefonicznym, kiedy centrala jest przeciążona, blokada dopuszczenia do sieci odbywa się poprzez brak emisji dźwięków wywołania.

Sztuką jest tu wytypowanie momentu, od którego dodawanie nowych obwodów wirtualnych naraża sieć na przeciążenie. W sieci telefonicznej jest to proste, ponieważ operuje ona na obwodach o z góry określonej prędkości transmisji (64 kb/s w przypadku nieskompresowanych danych dźwiękowych). Ale w sieciach komputerowych obwody wirtualne mogą definiować kanały o najróżniejszym zapotrzebowaniu na przepustowość. Każdy obwód powinien mieć więc przypisaną jakąś charakterystykę przenoszonego ruchu, inaczej trudno zarządzać dopuszczeniem do sieci.

Ruch jest często opisywany miarami prędkości i rozkładu. Sęk w dobraniu takiego opisu, który w prosty, ale znaczący sposób scharakteryzuje ruch w danym obwodzie — jest to problematyczne, ponieważ ruch pojawia się zazwyczaj w seriach mocno odbie-

gających od wartości średnich. Na przykład ruch związany z przeglądaniem strony WWW jest zupełnie inny niż ruch obsługujący strumieniowanie wideo i ten pierwszy trudniej scharakteryzować w długim okresie, ponieważ skumulowane serie ruchu WWW mogą łatwo doprowadzić do przeciążenia routerów w sieci. Powszechnie stosowaną miarą, która uwzględnia ten efekt, jest tzw. **cieknące wiadro** bądź **wiadro żetonów**. Operuje ona na dwóch parametrach, które reprezentują prędkość średnią ruchu i zwiększoną prędkość chwilową. Więcej o tych miarach powiemy w podrozdziale 5.4, przy okazji omawiania metod zapewniania jakości obsługi.

Uzbrojeni w deskryptory ruchu możemy w sieci decydować, czy dopuścić zestawienie nowego obwodu wirtualnego, czy nie. Sieć może na przykład rezerwować określoną pojemność wzdłuż ścieżek wykorzystywanych przez istniejące już obwody wirtualne, tak aby nie dopuścić do ich przeciążenia. W takim układzie deskryptor ruchu jest swego rodzaju umową świadczenia usługi — taką zarezerwowaną pojemność gwarantuje sieć. Przeciążenie jest wtedy niemożliwe. Zagłębiliśmy się jednak zanadto w temat jakości obsługi — wrócimy do niego w następnym podrozdziale.

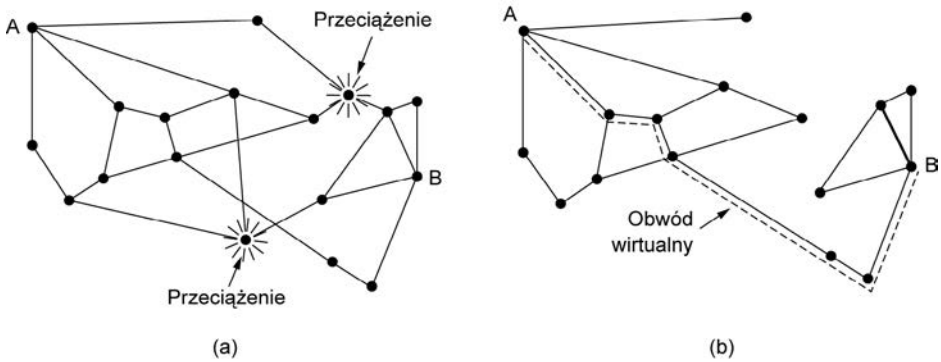
Nawet w przypadku braku gwarancji co do obwodu wirtualnego sieć wciąż może korzystać z danych zawartych w deskryptorze ruchu i decydować o dopuszczeniu do niej. Wystarczy oszacować, ile obwodów pomieści się w sieci bez ryzyka przeciążenia. Załóżmy, że obwody wirtualne przepychają ruch o szczytowej prędkości do 10 Mb/s wzdłuż tego samego 100-megabitowego łącza fizycznego. Ile takich obwodów można dopuścić? 10 obwodów na pewno nie przeciąży sieci, ale z drugiej strony tak mała ich liczba oznacza marnotrawstwo, ponieważ rzadko kiedy szczytowe natężenia ruchu dotyczą wszystkich obwodów w tym samym momencie. W faktycznych sieciach zbiera się statystyki opisujące dane typy transmisji i na ich podstawie szacuje się liczbę obsługiwanych obwodów wirtualnych — dzięki temu zyskujemy na efektywności sieci, jednak kosztem zwiększonego (ale wciąż akceptowalnego) ryzyka przeciążenia.

Dopuszczanie można też połączyć z routingiem z uwzględnieniem warunków ruchu, a więc z ustawieniem tras dla danego ruchu z pominięciem wąskich gardeł. Spójrzmy na przykład na sieć z rysunku 5.22 (a), w której przeciążone są dwa routery (oznaczone na rysunku).

Załóżmy, że host podłączony do routera A chce nawiązać połączenie z hostem podłączonym do routera B. Zwykle połączenie to przechodziłoby przez jeden z przeciążonych routerów. Aby uniknąć takiej sytuacji, możemy narysować sieć na nowo, jak na rysunku 5.22 (b), pomijając przeciążone routery i wszystkie ich linie. Linia przerywana przedstawia możliwą trasę dla obwodu wirtualnego, unikającą przeciążonych routerów. Tego rodzaju routing wrażliwy na obciążenie opisywał Shaikh i inni (1999).

5.3.4. Dławienie ruchu

W Internecie i w wielu innych sieciach komputerowych nadawcy dostosowują prędkość transmisji, tak aby wysłać możliwie dużą ilość danych, do maksimum dopuszczalnego pojemnością sieci. W takim układzie sieć z założenia pracuje w warunkach tuż



Rysunek 5.22. (a) Sieć z przeciążeniami, (b) Fragment sieci wolny od przeciążenia. W punkcie (b) został pokazany dodatkowo obwód wirtualny z A do B

poniżej punktu przeciążenia. Jeśli to przeciążenie jest już bardzo bliskie, sieć musi powiadomić nadawców o konieczności zdławienia ich transmisji i spowolnienia tempa wysyłania pakietów. Owa wskazówka jest traktowana jako sytuacja zwyczajna, nie zaś jako sytuacja wyjątkowa. Do opisu tego zachowania sieci stosuje się pojęcie **unikania przeciążenia** (ang. *congestion avoidance*) — dla odróżnienia tego momentu od stanu faktycznego przeciążenia sieci.

Przyjrzymy się kilku podejściom do realizacji pomysłu dławienia ruchu, nadającym się do stosowania zarówno w sieciach datagramowych, jak i w sieciach z obwodami wirtualnymi. Każde z opisywanych podejść łączy się z dwoma problemami. Przede wszystkim routery muszą potrafić określić moment zbliżającego się przeciążenia, najlepiej jeszcze zanim ono faktycznie nastąpi. W tym celu router musi stale monitorować zasoby używane do rozprowadzania ruchu. Dostępnymi tu miarami są zajętość łączy wyjściowych, rozmiar wewnętrznych buforów oczekujących na przetworzenie oraz liczba pakietów, które zostały utracone z powodu braku miejsca w buforach. Z tych trzech najbardziej istotny jest parametr drugi. Średnia zajętość łączy nie odpowiada wprost obciążeniu z powodu charakterystyki wielu transmisji (np. chwilowe szczyty transmisji): zużycie na poziomie 50% może oznaczać wartość niską przy gładkim ruchu o stałym natężeniu albo już zbyt wysoką dla ruchu o dużej zmienności natężenia. Z kolei liczba pakietów utraconych jest miarą dostępną zbyt późno — gdy dochodzi do tracenia pakietów na wejściu do routera, już można mówić o przeciążeniu sieci.

Tymczasem dobrym opisem przeciążenia jest opóźnienie kolejkowania pakietów do przetworzenia w routerach; przez większość czasu rozmiar kolejki powinien być mały, ale w przypadku pojawienia się chwilowych skoków natężenia ruchu od razu widać jej wydłużenie. Do wyznaczenia porządnej estymaty opóźnienia kolejkowania d można uokresowić próbkę chwilowej długości kolejki s i odpowiednio dostosowywać d — według wzoru:

$$d_{\text{nowe}} = d_{\text{stare}} + (1 - \alpha)s$$

gdzie stała α opisuje szybkość, z jaką router zapomina miary historyczne. Jest to tak zwana miara **EWMA** (*Exponentially Weighted Moving Average*), czyli krocząca średnia ważona wykładniczo. Wygładza ona fluktuacje i odpowiada działaniu dolnoprzepustowego filtra częstotliwości. Kiedy d przekracza wartość progową, router wykrywa stan bliski przeciążeniu.

Drugi problem do rozwiązania to potrzeba dostarczenia do odpowiednich nadawców powiadomień o konieczności zdławienia transmisji w momencie, kiedy jeszcze można zapobiec przeciążeniu. Samo przeciążenie jest odczuwalne w całej sieci, natomiast prewencja wymaga działań po stronie nadawców używających tej sieci. Dostarczenie zalecenia spowolnienia transmisji wymaga od routerów identyfikowania właściwych nadawców. Same ostrzeżenia powinny być też stosowane oszczędnie, bez zalewania pakietami ostrzegawczymi sieci stojącej u progu przeciążenia. Rozwiązań jest kilka.

Pakiety tłumienia

Najbardziej oczywistym sposobem powiadomienia nadawcy o rychłym przeciążeniu jest komunikacja bezpośrednia. W tej metodzie router wybiera nadawcę pakietów przeciążających i wysyła **pakiet tłumienia** (ang. *choke packet*) z powrotem do hosta źródłowego, podając mu cel transmisji znaleziony w pakiecie. Pierwotny pakiet może być oznaczony przez włączenie bitu w nagłówku, aby nie generował kolejnych pakietów tłumienia po drodze, a następnie zostaje przekazany dalej jak zwykle. W celu uniknięcia zwiększenia obciążenia sieci w czasie przeciążenia router może wysyłać pakiety tłumiące z małą prędkością.

Gdy host źródłowy otrzymuje pakiet tłumienia, wymaga się od niego redukcji ruchu wysyłanego do wskazanego celu, na przykład o 50%. W sieci datagramowej wybór nadawcy pakietów do zdławienia jest prosty — zwyczajne losowe próbkowanie oczekujących pakietów daje dużą szansę natrafienia na szybkiego nadawcę (jego pakietów jest stosunkowo dużo). Jest też równie prawdopodobne, że pakiety tłumiące trafią wtedy do tego samego nadawcy wielokrotnie. W takim przypadku powinien on ignorować kolejno spływające pakiety, póki odstęp między nimi mieści się w jakimś określonym przedziale czasu — tak aby mieć szansę doczekać efektów pierwszego zmniejszenia prędkości transmisji. Jeśli po tym okresie pakiety tłumiące wciąż spływają, nadawca powinien ponownie zmniejszyć prędkość transmisji, bo sieć wciąż jest przeciążona.

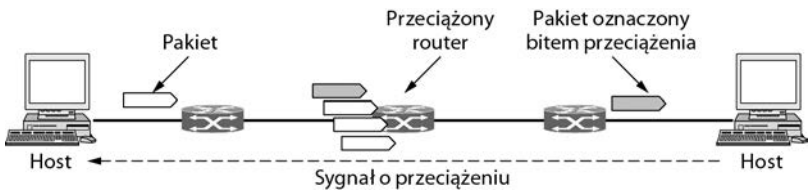
Przykładem pakietu tłumiącego z wczesnej fazy rozwoju sieci Internet jest komunikat `SOURCEQUENCH` (Postel, 1981). Nie przyjął się on jednak, po części z powodu braku jasnego określenia okoliczności, w których miał być generowany, i oczekiwanych działań po stronie odbiorcy pakietu. We współczesnym Internecie stosuje się alternatywne powiadomienia.

Jawne powiadamianie o przeciążeniach

Zamiast generować dodatkowe pakiety ostrzegające przed przeciążeniem, router może oznaczyć takim komunikatem dowolny rozprowadzany pakiet (odbywa się to poprzez ustawienie bitu w nagłówku pakietu). Kiedy sieć dostarczy pakiet, jego adresat może

zorientować się w sytuacji i poinformować o niej nadawcę w jednym z pakietów odpowiedzi (bądź potwierdzenia odbioru). Tak powiadomiony nadawca może wtedy przejść do dławienia swojej transmisji.

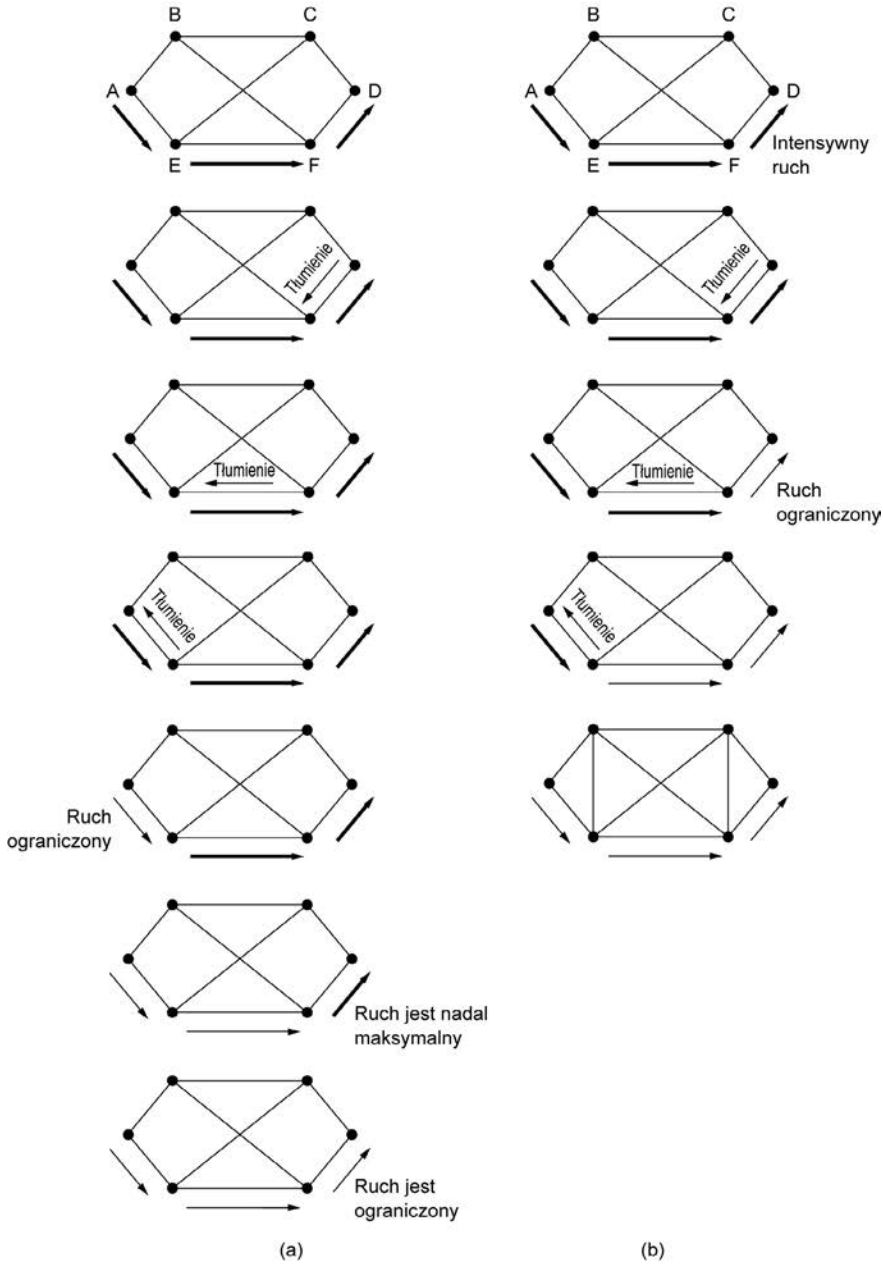
Schemat ten nosi miano *jawnego powiadamiania o przeciążeniu*, w skrócie **ECN** (od *Explicit Congestion Notification*), i jest stosowany w sieci Internet (Ramakrishnan i inni, 2001). Jest to udoskonalona wersja wczesnych protokołów sygnalizacji przeciążeń, przede wszystkim metody powiadamiania binarnego opracowanej przez Ramakrishnana i Jaina (1988), która była stosowana w architekturze sieci DECNET. W nagłówku pakietu IP zarezerwowano dwa bity przeznaczone do oznaczania pakietu pod przeciążeniem. Nadawca wysyła pakiety z bitami wyzerowanymi (jak na rysunku 5.23). Jeśli którykolwiek z routerów po drodze jest przeciążony, oznaczy pakiet bitem przeciążenia i rozprowadzi go do odbiorcy. Obowiązkiem adresata jest odpowiadać nadawcy z zachowaniem bitów odebranych z sieci, więc nadawca dowie się o przeciążeniu wraz z najbliższą odpowiedzią odbiorcy (np. wraz z pakietem potwierdzającym odebranie transmisji). Na rysunku sygnał o przeciążeniu jest zaznaczony linią przerywaną, ponieważ pojawia się na poziomie protokołu i pakietów IP (np. w transmisji TCP), a nie na poziomie właściwych danych wymienianych przez strony komunikacji. Nadawca transmisji po odebraniu od odbiorcy pakietów z ustawionymi bitami sygnalizacji przeciążenia powinien zareagować tak jak na pakiety tłumiące, czyli zdławić swoją transmisję.



Rysunek 5.23. Jawne powiadamianie o przeciążeniu

Tłumienie skok po skoku

Przy dużych szybkościach i długich dystansach po zasygnalizowaniu przeciążenia przez router nadawca może wysłać jeszcze wiele pakietów, a to z powodu opóźnienia, z jakim odbiera sygnał o przeciążeniu. Weźmy na przykład hosta z San Francisco (router *A* na rysunku 5.24), który wysyła transmisję do hosta w Nowym Jorku (router *D* z rysunku 5.24) z szybkością 155 Mb/s. Jeśli w hoście nowojorskim zacznie brakować buforów, to dotarcie pakietu tłumienia z powrotem do San Francisco, żądającego spowolnienia transmisji, zajmie około 40 milisekund. Sygnalizacja ECN zajmie jeszcze więcej czasu, ponieważ jest dostarczana do nadawcy za pośrednictwem adresata transmisji. Propagację pakietu tłumienia przedstawiają drugi, trzeci i czwarty krok z rysunku 5.24 (a). Podczas tych 40 ms zostało wysłanych kolejne 6,2 megabita danych. Nawet jeśli host w San Francisco natychmiast przestanie nadawać, te 6,2 megabita w kanale nadal będzie napływać i trzeba będzie sobie z nimi poradzić. Dopiero na siódmym schemacie z rysunku 5.24 (a) router z Nowego Jorku zauważy wolniejszy napływ danych.



Rysunek 5.24. (a) Pakiet tłumienia wpływający tylko na źródło transmisji, (b) Pakiet tłumienia wpływający na każdy węzeł, przez który przechodzi

Alternatywne rozwiązanie polega na tym, że pakiet tłumienia zaczyna działać już w każdym przeskoku, jak na rysunku 5.24 (b). Tutaj natychmiast po dotarciu pakietu tłumienia do *F* od tego routera żąda się redukcji przepływu do *D*. Będzie to wymagało poświęcenia przez *F* dodatkowych buforów na tę transmisję, ponieważ źródło nadal

pracuje na pełnych obrotach, lecz przynosi *D* natychmiastową ulgę (jak lekarstwo od bólu głowy z reklam telewizyjnych). W następnym kroku pakiet tłumienia dociera do *E*, co każe *E* ograniczyć przepływ do *F*. Zwiększa to zapotrzebowanie na bufory routera *E*, lecz natychmiast odciąża *F*. Na koniec pakiet tłumienia dociera do *A* i przepływ autentycznie maleje.

W sumie ten schemat tłumienia **skok po skoku** (ang. *hop-by-hop*) zapewnia szybkie odciążenie w punkcie przeciążenia kosztem zużycia dodatkowego miejsca w buforach w poprzednich węzłach na trasie transmisji. W ten sposób przeciążenie może zostać stłumione w zarodku bez tracenia jakichkolwiek pakietów. Pomysł ten opisuje Mishra i inni (1996).

5.3.5. Zrzut obciążenia

Gdy żadna z powyższych metod nie spowoduje zniknięcia przeciążenia, routery mogą wytoczyć ciężkie działa — **zrzut obciążenia** (ang. *load shedding*). To określenie jest eleganckim sposobem powiedzenia, że routery zalane pakietami, których nie są w stanie obsłużyć, po prostu wyrzucają te pakiety. Termin wziął się ze świata elektroenergetyki, gdzie oznacza rozmyślne odłączanie pewnych obszarów, aby uchronić całą sieć przed zapaścią w porach, gdy zapotrzebowanie na energię znacznie przekracza dostępne zasoby.

Zasadniczym pytaniem dla routera podlegającego przeciążeniu jest dobór odrzucanych pakietów. Wybór może być uzależniony od specyfiki aplikacji działających w danej sieci. W transferze plików stary pakiet ma większą wartość niż nowy, ponieważ odrzucenie pakietu nr 6 i zachowanie pakietów od 7 do 10 i tak wymusi po stronie odbiorcy buforowanie danych, których nijak nie może spożytkować bez odebrania brakującego pakietu. Z kolei w mediach czasu rzeczywistego nowy pakiet jest bardziej wartościowy niż stary, bo pakiety przeterminowane w aplikacjach czasu rzeczywistego są bezużyteczne.

Pierwsza zasada (starszy lepszy od nowego) nazywana jest często **winem**, a druga (świeży lepszy od starego) to **mleko** — wiadomo, że większość ludzi woli pić stare wino i świeże mleko niż na odwrót.

Bardziej inteligentne zrzucanie obciążenia wymaga współpracy z nadawcami. Przykładem mogą być pakiety przenoszące informacje dla routingu. Są one ważniejsze od zwyczajnych pakietów danych, bo dotyczą samych routerów, a więc i działania samej sieci. Jeśli zostaną utracone, sieć może stracić zdolność do rozprowadzania pakietów. Inny przykład to algorytmy kompresji wideo (jak MPEG), które okresowo przesyłają całą klatkę normalizującą, a następnie wysyłają kolejne klatki różnicowe względem ostatniej pełnej klatki. W tym przypadku odrzucenie pakietu niosącego informacje różnicowe będzie lepsze niż odrzucenie tego, który jest częścią pełnej klatki, gdyż przyszłe pakiety są od niego zależne.

Aby zaimplementować inteligentną zasadę odrzucania pakietów, aplikacje muszą oznaczać swoje pakiety, sygnalizując w ten sposób ich wartość. W takim układzie kiedy dojdzie do zrzutu obciążenia, routery będą w pierwszej kolejności odrzucać mniej ważne

pakiety, a pakiety ważniejsze będą odrzucane dopiero w ostateczności. Oczywiście wszyscy będą respektować zasady oznaczania pakietów i nikt nie pokusi się o oflagowanie wszystkich swoich transmisji znacznikiem: „BARDZO WAŻNY — NIE WYRZUCAĆ POD ŻADNYM POZOREM!".

Wymuszanie bądź zachęcanie do właściwego oznaczania pakietów odbywa się często na poziomie rozliczania za usługę. Na przykład sieć może dopuszczać transmisje z większą prędkością niż ta, za którą zapłacili nadawcy, jeśli w zamian ci będą oznaczać swoje pakiety znacznikiem niskiego priorytetu. Taka strategia jest niegłupia, ponieważ pozwala znacznie skuteczniej wykorzystać bezczynne zasoby. Hosty mają prawo ich używać, dopóki nikt inny nie jest nimi zainteresowany, lecz bez nabywania prawa do nich w okresach dużego obciążenia.

Random Early Detection

Wiadomo, że obsługa przeciążenia u jego zarania jest bardziej skuteczna niż wtedy, gdy pozwolimy mu narobić bigosu i dopiero wtedy będziemy próbować sobie z nim poradzić. To spostrzeżenie prowadzi do ciekawego ulepszenia metody zrzutu obciążenia, w ramach którego pakiety są odrzucane, jeszcze zanim dojdzie do wyczerpania miejsca w buforach.

Chodzi o to, że większość hostów w sieci Internet nie otrzymuje jeszcze sygnałów o przeciążeniu w postaci ECN; w wielu regionach sieci jedynym niezawodnym sygnałem przeciążenia jest utrata nadawanych pakietów. Trudno przecież zbudować taki router, który nie gubi pakietów w warunkach przeciążenia. Protokoły transportowe (takie jak TCP) są więc projektowane z założeniem, że utrata pakietów świadczy o przeciążeniu i spowalnianiu źródła transmisji. Do zastosowania takiej metody doprowadziło rozumowanie, że TCP został zaprojektowany dla sieci kablowych, które są bardzo niezawodne, więc pakiety tracą się głównie z powodu przepełnienia buforów, a nie błędów transmisji. W łączach bezprzewodowych dobra współpraca z TCP wymusza zatem odzysk błędów transmisji na poziomie warstwy łącza danych (nie są więc one widoczne w warstwie sieciowej).

Można to wykorzystać do walki z przeciążeniami. Odrzucanie przez routery pakietów, jeszcze zanim sytuacja stanie się beznadziejna, oznacza, że jest czas na podjęcie działań po stronie nadawcy, zanim będzie za późno. Popularny służący do tego algorytm nosi nazwę **RED** (*Random Early Detection* — **losowe wczesne wykrywanie**) (Floyd i Jacobson, 1993). Aby zdecydować, kiedy przychodzi pora, by zacząć odrzucać pakiety, routery rejestrują na bieżąco średnią wartość długości swoich kolejek. Gdy średnia długość kolejki dla jakiegoś łącza przekracza ustaloną granicę, uznaje się, że łącze jest przeciążone, i losowo odrzuca małą część pakietów. Losowy wybór pakietów jest optymalny, ponieważ w sieci datagramowej router nie jest w stanie wytypować źródła przeciążenia. Każdy z nadawców, którego dotyczyła utrata pakietów, dowie się o niej w wyniku braku potwierdzenia od odbiorcy, i wtedy sam spowolni swoją transmisję. Utrata pakietu jest tu więc odpowiednikiem dostarczenia pakietu tłumiącego, ale w sposób niejawny.

Routery RED cechują się lepszą wydajnością w porównaniu do routerów, które odrzucają pakiety dopiero po przepełnieniu buforów, choć uzyskanie optymalnych efektów wymaga pewnego dostrojenia. Na przykład idealna liczba pakietów do odrzucenia jest zależna od tego, ilu nadawców zamierzamy powiadomić o przeciążeniu. Mimo to preferowaną opcją jest sygnalizacja ECN (jeśli tylko jest możliwa). Działa podobnie, ale dostarcza sygnał o przeciążeniu w sposób jawny, a nie poprzez wnioskowanie z utraty pakietów; RED stosuje się tam, gdzie hosty sieci nie obsługują sygnalizacji jawnej.

SKOROWIDZ

B

C

D

E

F

G

H

K

L

Ł

M

N

O

P

Q

R

S

Ś

T

U

V

W

X

Z

Ż

Technika przesyłania danych rozwija się w zawrotnym tempie. Co rusz wprowadzane są nowe standardy, protokoły i narzędzia. Od czasu ukazania się na rynku czwartego wydania tej książki szczególnie mocno rozwinęły się wszystkie obszary związane z sieciami bezprzewodowymi. Mobilny dostęp do internetu jest w dzisiejszych czasach normą, dlatego znajomość nowych trendów oraz biegłość w poruszaniu się w gąszczu specjalistycznej wiedzy są koniecznie potrzebne wszystkim projektantom i administratorom.

LOW-EARTH ORBIT SATELLITE

Piąte wydanie książki ***Sieci komputerowe*** pozwoli Ci na błyskawiczne opanowanie najbardziej aktualnej wiedzy. Autor położył tu szczególny nacisk na sieci bezprzewodowe — standardy 802.11, 802.16, Bluetooth™ oraz dostęp przez sieć komórkową zostały dogłębnie omówione. Lektura tej pozycji umożliwi Ci również uzyskanie kompletnej wiedzy na temat tradycyjnych sieci kablowych. To medium transmisji jeszcze długo będzie wykorzystywane tam, gdzie jest wymagana najwyższa niezawodność. Ta książka jest idealnym wprowadzeniem do sieci współczesnych — *oraz tych, które dopiero powstaną*.

Przeczytaj i sprawdź:

- jakie są dostępne media transmisyjne
- co warto wiedzieć o zaletach i wadach protokołów routingu
- w jaki sposób zapewnić wydajność sieci (QoS)
- jak zagwarantować bezpieczeństwo przesyłanych danych

Andrew Stuart Tanenbaum

– profesor informatyki, zdobywca prestiżowego European Research Council Advanced Grant na badania nad niezawodnością w systemach komputerowych. Autor bardzo znanych i cenionych książek informatycznych, które stanowią lekturę obowiązkową w dziedzinie komputerów.

David J. Wetherall

– profesor informatyki, od ponad dwudziestu lat zajmujący się sieciami komputerowymi. W kręgu jego zainteresowań badawczych znajdują się protokoły internetowe, sieci bezprzewodowe i bezpieczeństwo komunikacji.

Obowiązkowa lektura każdego administratora i projektanta sieci komputerowych!

Informatyka w najlepszym wydaniu

Cena 129,00 zł

ISBN 978-83-246-3079-0

9 788324 630790