УДК 004.77:621.39

О.О. Можаєв[1], Н.Х. Раковська[2], С.Г. Семенов[1]

[1] *Національний технічний університет «ХПІ», Харків*
[2] *Харківський університет Повітряних Сил імені Івана Кожедуба, Харків*

МЕТОД ПІДВИЩЕННЯ ОПЕРАТИВНОСТІ ІНФОРМАЦІЙНОГО ОБМІНУ З «ХМАРНИМИ» АНТИВІРУСНИМИ СИСТЕМАМИ

У статті розроблено метод підвищення оперативності інформаційного обміну з ресурсами «хмарних» антивірусних систем, що відрізняється від відомих введенням додаткових умов обробки високопріоритетних інформаційних пакетів в справедливих алгоритмах розподілу обчислювальних і телекомунікаційних ресурсів. Сформульована загальна оптимізаційна задача підвищення оперативності передачі даних.

Ключові слова: *інформаційний обмін, комутаційне обладнання, «хмарні» антивірусні системи.*

Вступ

Постановка завдання. В останні роки підвищення інтенсивності інформаційного трафіку в комп'ютерних мережах змусило розробників телекомунікаційного обладнання використовувати різні механізми, що мають мету оптимізації існуючих ресурсів.

Одним з напрямків вирішення поставлених перед розробниками завдань є впровадження сучасних алгоритмів управління чергами в комутаційному обладнанні (маршрутизаторах). Найбільш перспективним з них є алгоритм WF2Q [1], характерною особливістю якого є принцип справедливого розподілу мережевих ресурсів (буфера пам'яті, пропускної спроможності). Проведені дослідження показали, що використання такого підходу розподілу мережевих ресурсів дає позитивний результат в нормальних умовах функціонування комп'ютерних і телекомунікаційних систем. Однак, в нештатних ситуаціях, коли необхідно використовувати зовнішні ресурси «хмарних» антивірусних систем [2] і забезпечувати оперативну обробку і доставку спеціальних сигнатур (метаданих), використання підходу справедливого розподілу мережевих ресурсів неефективно. У цих умовах завдання підвищення оперативності передачі спеціальних сигнатур в «хмар-

ні» антивірусні системи шляхом удосконалення існуючих походів розподілу мережевих ресурсів стає актуальним. Аналіз [3] показав, що для вирішення завдань підвищення оперативності обміну доцільно використовувати ряд підходів, пов'язаних з розподілом ресурсів на умовах відносної пріоритезації і резервування ресурсів для кожної черги (найбільш пріоритетним класом пропонується вважати інформаційний трафік з жорсткими вимогами до часу доставки інформаційних пакетів). У зазначених умовах оптимізаційну задачу підвищення оперативності обміну можна представити у вигляді виразів:

$$N \cdot \overline{T}_{обс}^{[max]} \to \min, \quad J^{[i]} \le J_{доп}^{[i]}, \qquad (1)$$

де $\overline{T}_{обс}^{[max]}$ – середній час обслуговування одного високопріоритетного пакета, при цьому, час обслуговування одного пакета і-ї черги обчислюється за такою формулою: $T_{обс}^{[i]} = T_{кон}^{[i]} - T_{пост}^{[i]}, i = \overline{1..N}$, $T_{кон}^{[i]}$ – час завершення обслуговування пакета в і-й черзі, $T_{пост}^{[i]}$ – час надходження пакета в і-ту чергу, N – кількість черг в системі, $J^{[i]}$ – джіттер часу обслуговування пакетів в і-й черзі, $J_{доп}^{[i]}$ – максимально допустиме значення джиттера часу обслуговування пакетів для і-ої черги.

При цьому часткові обмеження досліджуваної системи можна представити у вигляді виразів:

$$T_{нач}^{[max]} \to \min, \quad \overline{T}_{обс}^{[max]} \to \min, \quad \overline{T}_{обс}^{[j]} \le T_{доп}^{[j]}, \qquad (2)$$

де $T_{нач}^{[max]}$ – час початку обробки першого високопріоритетного [max] пакета, $\overline{T}_{обр}^{[j]}$ – середній час обслуговування невисокопріоритетного пакета $j = \overline{1..N-1}$, $T_{доп}^{[j]}$ – максимально допустимий час обслуговування пакетів (згідно з вимогами критерію якості обслуговування пакетів TCP / IP) для j-ої черги.

Вдосконалений алгоритм управління обчислювальними і телекомунікаційними ресурсами

Для вирішення поставленої оптимізаційної задачі підвищення оперативності передачі даних пропонується вдосконалити алгоритм управління чергами. В основу розглянутого вдосконаленого алгоритму управління чергами покладено спосіб розрахунку віртуального часу обслуговування інформаційних пакетів, що відрізняється від відомих урахуванням фактора передачі сигнальних даних з комп'ютерних мереж в «хмарні» антивірусні системи. При цьому зазначені сигнальні дані отримують найвищий пріоритет обробки у вузлах комутації ($N_{приор} = 8$, де $N_{приор}$ - номер пріоритету, присвоєний інформаційному пакету).

На першому кроці вдосконаленого алгоритму управління чергами з інформаційного потоку вибирається перший (еталонний) пакет, з деяким $N_{приор}$, а також значенням віртуального часу обслуговування в черзі – VTT.

На другому кроці проводиться порівняння «еталонного» інформаційного пакета з іншими доступними станом на даний момент часу. При цьому рішення про присвоєння «еталонного» пріоритету інформаційного пакету приймається за наступними критеріями: мінімальне значення віртуального часу обслуговування в черзі ($VFT = \min$); приналежність інформаційного пакета до черги з максимальним пріоритетом. При цьому друга умова присвоєння «еталонного» пріоритету виконується не в повному обсязі, а з деякими винятками, обумовленими показником $P_{присв}$ - імовірності присвоєння пріоритету ($P_{присв} = 0,5$, $P_{присв} = 0,7$, $P_{присв} = 0,9$), що задається адміністратором комп'ютерної мережі шляхом відповідних налаштувань в інтелектуальних вузлах комутації. Одним з невирішених завдань залишається задача оптимального розподілу обчислювальних та інформаційних ресурсів (наприклад, полоси пропускання), що дозволяє мінімізувати час виявлення зловмисного програмного забезпечення. Дану задачу пропонується вирішити за допомогою імітаційного моделювання, при цьому параметри, які необхідно використовувати під час оптимального розподілу полоси пропускання комп'ютерної мережі, обрано такі [4]: N = 10000, RTT = 100 мс, P = 10 Гбит/с, $B \approx \frac{10^9 \cdot 10^{-1}}{\sqrt{10000}} = 10^6 = 1.25$ Мб/с, де $B \approx \frac{P \cdot RTT}{\sqrt{N}}$ – об'єм буфера маршрутизатора, N - число незалежних потоків трафіку, P - пропускна здатність каналу, RTT (Round Trip Time) - час проходження сигналу від джерела трафіку до маршрутизатора і назад.

При розмірі одного пакета 1024 байт для технології Ethernet отримуємо, що об'єм буфера маршрутизатора ~ 1000 пакетів.

Оцінка ефективності методу підвищення оперативності передачі спеціальних сигнатур в «хмарні» антивірусні системи

Для оцінки ефективності методу підвищення оперативності передачі спеціальних сигнатур в «хмарні» антивірусні системи можна використовувати різні підходи розподілу телекомунікаційних ресурсів: статичний (несправедливий) розподіл, який суттєво зменшує середній час і джіттер часу обробки інформаційних пакетів виділеного (максимального) рівня пріоритетності, але при цьому порушується режим забезпечення якості обслуговування інформаційних пакетів

інших пріоритетів; принципи справедливого розподілу на основі обчислення вагового коефіцієнта ω_i:

$$\omega_i = \sqrt{i} \Big/ \sum_{j=1}^{N} \sqrt{j}, \quad N = 8, i = \overline{1..N}, \qquad (3)$$

$$\omega_i = i \Big/ \sum_{j=1}^{N} j, \quad N = 8, i = \overline{1..N}, \qquad (4)$$

$$\omega_i = i^2 \Big/ \sum_{j=1}^{N} j^2, \quad N = 8, i = \overline{1..N}, \qquad (5)$$

$$\omega_i = e^i \Big/ \sum_{j=1}^{N} e^j, \quad N = 8, i = \overline{1..N}, \qquad (6)$$

які частково або повністю вирішують проблеми несправедливого розподілу.

Так використання принципу справедливого розподілу обчислювальних і телекомунікаційних ресурсів відповідно до виразів (3) – (6) дозволило до 5 разів знизити час обробки інформаційних пакетів у порівнянні з алгоритмом WF2Q. Однак у випадках використання підходів на основі виразів (3), (5), вимоги до часу обробки і джиттера часу обробки інформаційних пакетів окремих рівнів пріоритетності в заданих при дослідженні умовах не забезпечуються.

Таким чином, аналіз результатів математичного моделювання дозволяє зробити висновок про недоцільність використання наступних варіантів розподілу інформаційних пакетів: статичний розподіл; справедливий розподіл у відповідності з виразом (3); справедливий розподіл у відповідності з виразом (5).

У той же час справедливий розподіл відповідно до виразів (4) і (6) в повному обсязі задовольняє умовам, заданим в завданні (1) – (2). При цьому, однак, слід зауважити, що результати використання алгоритму WFQI відповідно до виразу (6) показали результати, близькі до максимально допустимих, що дозволяє зробити висновок щодо використання даного підходу тільки у випадках, коли система працює в незавантаженому стані (~10 – 20% від середньо-добового завантаження). Проведені дослідження показали доцільність використання удосконалених алгоритмів розподілу обчислювальних і телекомунікаційних ресурсів в методі підвищення оперативності інформаційного обміну з «хмарними» антивірусними системами. При цьому використання даного методу передбачає ряд змін в протоколах інформаційного обміну і попередніх налаштувань в комутаційному обладнанні комп'ютерних мереж. Надалі доцільно провести додаткові дослідження з метою охоплення максимального спектра можливих початкових умов моделювання і, відповідно, виявлення основних тенденцій зміни показників.

Висновок

Таким чином, розроблено та досліджено метод підвищення оперативності передачі спеціальних сигнатур в «хмарні» антивірусні системи, одним із складових елементів якого є вдосконалений алгоритм WFQI розподілу обчислювальних і телекомунікаційних ресурсів. Результати порівняльних експериментів показали ефективність розробленого методу, який дозволяє в середньому до 5 разів зменшити час передачі спеціальних сигнатур в «хмарні» антивірусні системи.

Список літератури

1. Кучерявый Е.А. Управление трафиком и качество обслуживания в сети Интернет / Е.А. Кучерявый. – СПб.: Наука и Техника, 2004. – С. 150-188.

2. Семенов С.Г. Методика настройки параметров распределения доступа и защиты информации в компьютерных системах критического применения / С.Г. Семенов // Системи озброєння і військова техніка. – Х.: ХУ ПС. – 2012. – Вип. 4(32). – С. 153-158.

3. Кучук, Г.А. Моделювання трафіка мультисервісної розподіленої телекомунікаційної мережі / Г.А .Кучук, І.Г. Кіріллов, А.А .Пашнєв // Системи обробки інформації. – Х.: ХУ ПС, 2006. – Вип. 9 (58). – С. 50-59.

4. 5RFC 791 – Internet Protocol. [Електронний ресурс]. – Режим доступу до матеріалів протоколу : http://www.faqs.org/rfcs/rfc791.html/.

Надійшла до редколегії 28.06.2014

Рецензент: д-р техн. наук, проф. С.Г. Удовенко, Харківський національний університет радіоелектроніки, Харків.

МЕТОД ПОВЫШЕНИЯ ОПЕРАТИВНОСТИ ИНФОРМАЦИОННОГО ОБМЕНА С «ОБЛАЧНЫМИ» АНТИВИРУСНЫМИ СИСТЕМАМИ

А.А. Можаев, Н.Х. Раковская, С.Г. Семенов

В статье разработан метод повышения оперативности информационного обмена с ресурсами «облачных» антивирусных систем, отличающийся от известных введением дополнительных условий обработки высокоприоритетных информационных пакетов в справедливых алгоритмах распределения вычислительных и телекоммуникационных ресурсов. Сформулирована общая оптимизационная задача повышения оперативности передачи данных.

Ключевые слова: *информационный обмен, коммутационное оборудование, «облачные» антивирусные системы.*

A METHOD FOR INCREASING THE EFFICIENCY OF INFORMATION EXCHANGE WITH THE "CLOUD" ANTI-VIRUS SYSTEMS

A.A. Mozhaev, N.H. Rakovskaya, S.G. Semenov

The method of expediting information exchange with resources of "cloud" anti-virus systems is developed in the paper. The method is varies from the known ones with introduction of additional conditions for processing of high-priority information packets in fair scheduling algorithms for computer and telecommunication resources.

Keywords*: information exchange, switching equipment, "cloud" anti-virus system.*