

Ю. М. МОНаХОВ

РАСПРЕДЕЛЕННЫЙ МЕХАНИЗМ УПРАВЛЕНИЯ ПЕРЕГРУЗКАМИ В СЕТИ ПЕРЕДАЧИ ДАННЫХ

Проанализированы равновесные состояния системы управления трафиком протокола TCP. Предложен новый способ управления перегрузками TCP/IP-сети, отличительной особенностью которого является медленная адаптация и возможность выборочного изъятия пакетов из очереди.

Ключевые слова: TCP/IP, вычислительная сеть, перегрузки, AQM, управление.

Передача данных между конечными системами в пакетно-ориентированной сети, основанной на стеке TCP/IP, происходит за счет использования фиксированных и переменных сегментов ограниченного размера. Обычно перегрузки в пакетно-ориентированных сетях носят локальный характер, и механизм управления перегрузками используется, чтобы улучшить общую сетевую производительность сети, регулируя локальные ситуации на маршрутизаторах. Контроль перегрузки осуществляется через управление скоростью передачи потоков данных каждого источника исходя из текущего уровня загрузки сети [1]. Применение таких механизмов контроля не только позволяет справиться с перегрузками, но также приводит к более эффективному использованию доступной полосы пропускания. Этот подход ограничен, в силу того что информация о текущем состоянии сети должна доставляться по той же (перегруженной) сети передачи данных (СПД). В момент перегрузки доставка такой информации затруднена и замедлена, и поэтому узлы не получают данных об актуальном состоянии сетевой инфраструктуры [2, 3]. Это несколько ограничивает сетевую производительность всех схем управления перегрузками, основанных на таком подходе.

Для того чтобы формально описать процесс управления перегрузкой, необходимо сначала установить основные зависимости между параметрами внутри самого протокола TCP, а именно размером окна фрагментации и очередью.

Динамику этих параметров можно с необходимой точностью описать системой дифференциальных уравнений:

$$\begin{cases} \frac{dw}{dt} = \frac{a - \left(a + \frac{2b}{2-b}w\right)wp}{t_{RTT}}, \\ \frac{dq}{dt} = \frac{Nw}{t_{RTT}}, \\ t_{RTT} = \frac{q}{C} + T_p, \end{cases} \quad (1)$$

где w — размер окна фрагментации, q — длина очереди, p — вероятность ECN-маркинга (или удаления) пакетов, a — параметр протокола *TCP Increase*, b — параметр протокола *TCP Decrease*, N — число источников пакетов, C — пропускная способность канала, t_{RTT} — время между отправкой запроса и получением ответа, T_p — средняя задержка.

Так как AQM-схемы управления перегрузками работают преимущественно с очередью EWMA-усредненной длины [4], то необходимо проследить и ее динамику:

$$\frac{d\bar{q}}{dt} = \omega_q (q - \bar{q}); \quad p = p_{\max} \frac{q - th_{\min}}{\Delta th}; \quad \Delta th = th_{\max} - th_{\min}, \quad (2)$$

где ω_q — частота низкочастотного фильтра, \bar{q} — средняя длина очереди, p_{\max} — максимальная вероятность ECN-маркинга (или удаления) пакетов, th_{\min} и th_{\max} — минимально и максимально допустимая длина очереди соответственно.

EWMA (Exponential Weighted Moving Average) — метод усреднения, использующий следующее рекуррентное соотношение:

$$\bar{q}_n = (\bar{q}_{n-1} (1 - 2^{-\gamma})) + (2^{-\gamma} q), \quad (3)$$

где γ — весовой коэффициент.

В AQM-схемах управляемым параметром является максимальная вероятность удаления (маркинга) пакетов.

Проанализировав систему (1) и управляющее воздействие (2), найдем ее равновесное состояние, т.е. вектор параметров $(\mathbf{w}, \mathbf{q}, \bar{\mathbf{q}}, \mathbf{p}, \mathbf{p}_{\max})$, оптимальных для функционирования СПД. При этом значение оптимальной средней длины очереди $\bar{\mathbf{q}}$ выступает в качестве начального условия, т.е. задается в процессе администрирования или внедрения системы контроля перегрузок:

$$\mathbf{w} = \frac{\bar{\mathbf{q}} + T_p C}{N}, \quad (4)$$

$$\mathbf{q} = \bar{\mathbf{q}} \text{ (н.у.)}, \quad (5)$$

$$\mathbf{p} = \frac{(2 - b)aN^2}{(\bar{\mathbf{q}} + T_p C)(2b(\bar{\mathbf{q}} + T_p C) + (2 - b)aN)}, \quad (6)$$

$$\mathbf{p}_{\max} = \frac{\Delta th(2 - b)aN^2}{(\bar{\mathbf{q}} + T_p C)(\bar{\mathbf{q}} - th_{\min})(2b(\bar{\mathbf{q}} + T_p C) + (2 - b)aN)}. \quad (7)$$

Характер зависимости между вероятностью ECN-маркинга пакета и средней длиной очереди можно установить, изучив *следствия* из равенств (6) и (7).

Следствие 1. Значение \mathbf{p}_{\max} не определено для $\bar{\mathbf{q}} = th_{\min}$, т.е.

$$\lim_{\bar{\mathbf{q}} \rightarrow th_{\min}} \mathbf{p}_{\max} = +\infty. \quad (8)$$

Следствие 2. Если $\bar{\mathbf{q}} > th_{\min}$, то $\mathbf{p}_{\max} \sim \frac{1}{\bar{\mathbf{q}}}$ и

$$\lim_{\bar{\mathbf{q}} \rightarrow \infty} \mathbf{p}_{\max} = 0. \quad (9)$$

Обратно пропорциональная зависимость указывает на возможность построения простого адаптивного механизма, зависящего только от текущего значения средней длины очереди \bar{q} . Например, если текущая средняя длина очереди меньше оптимальной, то \mathbf{p}_{\max} необходимо уменьшить на некоторую величину (или в некоторое число раз); и наоборот, если \bar{q} больше оптимальной, то \mathbf{p}_{\max} необходимо увеличить. Такой базовый алгоритм адаптации показан на рис. 1.

Обозначим величину декремента и инкремента p_{\max} как α и β соответственно. Допустим, что средняя длина очереди считается оптимальной, пока находится в интервале $[th_{\min}, th_{\max}]$. Тогда базовый алгоритм адаптивной AQM-схемы будет выглядеть так, как показано на рис. 1, б.

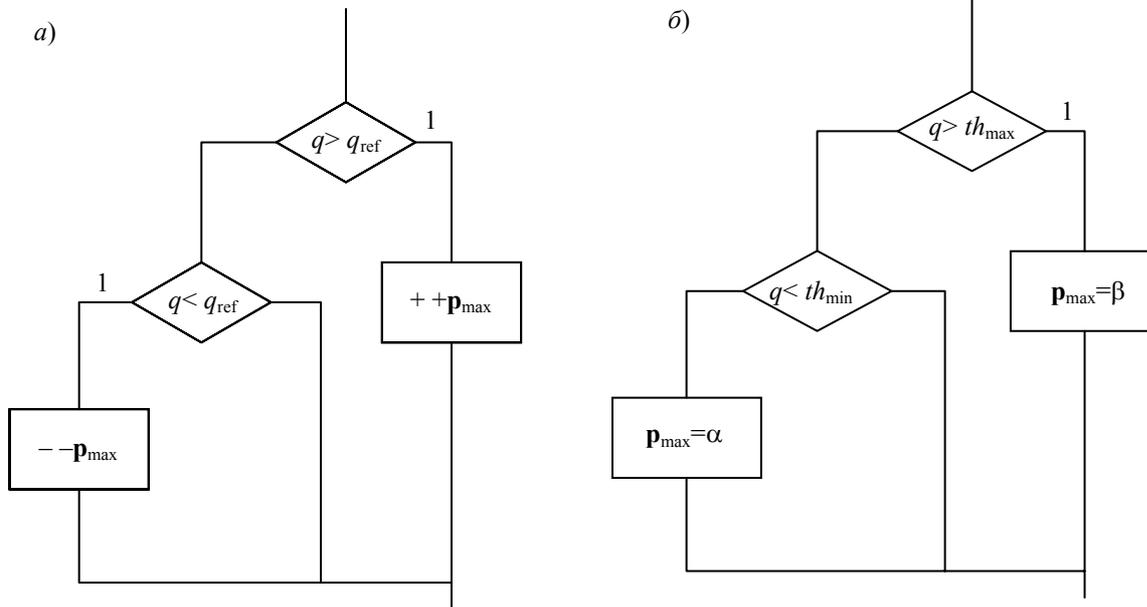


Рис. 1

Отметим, что в разных вариантах подобных адаптивных алгоритмов предельная вероятность p_{\max} может изменяться как линейно, так и полиномиально и экспоненциально [5, 6]. Был выбран линейный характер изменения p_{\max} , чтобы протокол TCP мог корректно обработать алгоритм *slow start*.

В настоящей работе предлагается способ управления перегрузками, обладающий следующими отличительными особенностями:

- сигнатурный анализ пакетов для предотвращения информационных атак, т.е. все пакеты, соответствующие сигнатуре, поступившей из центра управления, удаляются из очереди;
- обеспечение ECN-маркинга пакетов как более эффективного способа сигнализирования о перегрузке;
- централизация процедуры выбора управляющих параметров на основе анализа сети отдельным блоком сенсоров трафика;
- медленная адаптация с целью избежания монополизации каналов и глобального увеличения фрагментации ввиду TCP-коллизий.

При таком методе управления перегрузками помимо алгоритма удаления пакетов используется протокол взаимодействия агентов и центра управления, оптимизированный под высокие нагрузки на СПД [7, 8].

Система, позволяющая реализовать способ, состоит из центра контроля перегрузок (ЦКП), агентов контроля перегрузок (АКП) и промежуточного мультиплексора (Mux) — демультимплексора (Demux), снижающего нагрузку на маршрутизаторы подсетей (рис. 2). Каждый компонент обладает ограниченным набором возможных действий, на которых и основывается протокол обмена данными.

ЦКП осуществляет следующие действия:

- пуск АКП;
- останов АКП;
- посылка контролирующего пакета, содержащего параметры алгоритма управления перегрузкой;
- посылка сигнатур вредоносных пакетов.

- АКП помимо обработки адаптивного алгоритма осуществляет отправку
- сообщения о статусе (метка Вкл./Ожидание);
 - информации об управляемом параметре — максимальной длины очереди;
 - информации о числе пакетов, удаленных из очереди.

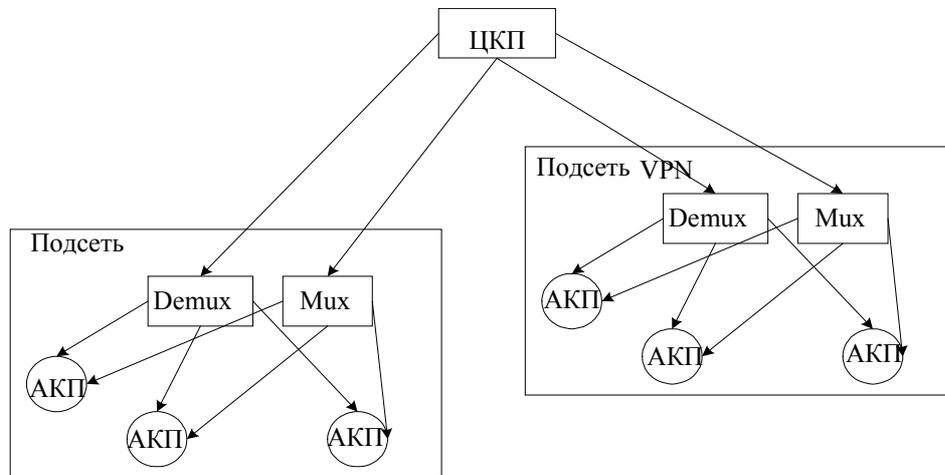


Рис. 2

Указанные действия инициируются ЦКП путем рассылки агентам управляющих пакетов. При этом благодаря мультиплексированию данных через маршрутизатор подсети проходит лишь один управляющий пакет. Рассмотрим этот протокол обмена более подробно.

1. Пуск/останов АКП

На данном шаге участвуют четыре типа пакетов: OS-REQ (On/Standby Request) — запрос пуска-останова всех АКП подсети, OS-ANS (On/Standby Answer) — результат пуска-останова всех АКП подсети, OS-REQD (Demuxed) — запрос пуска-останова одного АКП подсети, OS-ANS D — результат его пуска или останова. Через маршрутизатор проходят только пакеты OS-REQ и OS-ANS. Обмен пакетами OS-REQD и OS-ANS D осуществляется в рамках одной TCP-сессии.

2. Контролирующий запрос/ответ

На данном этапе происходит обмен параметрами алгоритма управления перегрузкой. Для этого вводится структура CTLPACK размером шесть октетов, содержащая пять полей, соответствующих параметрам α , β , th_{max} , th_{min} и q_{ref} . Для возможности повышения точности в будущем резервируется дополнительный октет. Обмен на данном шаге также использует четыре типа пакетов: CTL-REQ (Control Request) — поставка параметров алгоритма всем АКП подсети, CTL-ANS (Control Answer) — мультиплексированный результат поставки параметров, содержащий максимальные вероятности ECN-маркинга (p_{max}) для всех АКП подсети, CTL-REQD и CTL-ANS D — то же, но для одного АКП. В свою очередь, возможна отправка самопроизвольных CTL-ANS D-пакетов с некой регулируемой частотой (авторами предлагается посылать такие пакеты один раз в секунду) с целью обеспечить оперативное отслеживание состояния сети центром контроля перегрузок.

СПИСОК ЛИТЕРАТУРЫ

1. Stevens W. TCP Slow Start, Congestion Avoidance, Fast Retransmit, and Fast Re-covery Algorithms // RFC. 1997. January. 2001 p.
2. Paxson V., Allman M., Dawson S., Fenner W., Griner J., Heavens I., Lahey K., Semke J., Volz B. Nown TCP Implementation Problems // RFC. 1999. March. 2525 p.
3. Paxson V. End-to-End Internet Packet Dynamics // Proc. SIGCOMM '97. Cannes, France, 1997.

4. *Mathis M., Mahdavi J.* Forward Acknowledgment: Refining TCP Congestion Control // Proc. SIGCOMM'96. Stanford, CA, 1996.
5. *Монахов Ю. М.* Динамика протокола TCP в условиях сетевых атак и перегрузок // Математические методы в технике и технологиях ММТТ-21. Сб. тр. XXI Междунар. науч. конф. Секция 6 / Под общ. ред. В. С. Балакирева. Саратов: Сарат. гос. техн. ун-т, 2008. Т. 7. С. 264.
6. *Монахов Ю. М.* Уязвимости протокола транспортного уровня TCP // Алгоритмы, методы и системы обработки данных / Под ред. С. С. Садыкова, Д. Е. Андрианова. М.: Горячая линия – Телеком, 2006. С. 203—210.
7. *Монахов Ю. М., Макаров Р. И.* Автоматизированная система обнаружения аномального функционирования распределенной вычислительной среды АСУ // Системный анализ: теория и практика. 2009. № 3. С. 86—89.
8. *Монахов Ю. М.* Использование fuzzy-модели для описания и предсказания поведения сети передачи данных в условиях атак типа „отказ в обслуживании“ // Горный информационно-аналитический бюллетень. 2008. № 10. С.133—137.

Сведения об авторе

Юрий Михайлович Монахов — канд. техн. наук, доцент; Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра информатики и защиты информации;
E-mail: unclcfck@gmail.com

Рекомендована ВЛГУ

Поступила в редакцию
17.04.12 г.