УДК 681.14

МЕТОДЫ И СРЕДСТВА ЭФФЕКТИВНОГО УПРАВЛЕНИЯ ПЕРЕДАЧЕЙ ДАННЫХ В ЗАЩИЩЕННЫХ КОМПЬЮТЕРНЫХ СЕТЯХ

В.Е. МУХИН, ЛУАЙ ДАРВИШ

Выполнен анализ современных средств управления передачей данных в компьютерных сетях на основе протокола TCP/IP. Разработан новый метод раннего приостановления передачи пакетов, базирующийся на принципе активного управления очередями пакетов в маршрутизаторах и серверах, и на его основе предложены средства предотвращения перегрузок трафика в защищенных компьютерных сетях. Проведенные исследования средств предотвращения перегрузок в компьютерных сетях подтвердили повышение эффективности предлагаемых методов и средств по сравнению с существующими, что особенно важно в практических приложениях для реализации сетевых сервисов.

ВВЕДЕНИЕ

Проблемы обеспечения безопасности информации, обрабатываемой и передаваемой в компьютерных сетях (КС), являются весьма актуальными. Средства защиты — неотъемлемая часть большинства современных КС, особенно при обработке критичной и ценной информации, доступ к которой необходимо ограничить. На нынешнем этапе развития информационных технологий возникает специфическое противоречие в использовании средств защиты информации в КС: механизмы защиты информации должны обеспечивать требуемый уровень защищенности обрабатываемых данных, при этом средства защиты не должны существенно снижать общую пропускную способность пользовательской информации в КС.

Один из ключевых механизмов защиты информации в КС — средства аутентификации субъектов и сообщений, позволяющие гарантировать подлинность пользователей КС, обменивающихся информацией, а также целостность самой информации [1]. Надежные схемы аутентификации базируются на применении специализированного сервера безопасности КС, который, помимо реализации комплекса функций защиты информации, непосредственно выступает основным элементом механизма аутентификации [2].

В процессе реализации протокола аутентификации пользователи КС обмениваются между собой сообщениями для установления подлинности друг друга и гарантирования целостности передаваемой информации. При этом все пользователи КС отправляют запросы к серверу безопасности. С ростом числа пользователей КС канал сервера может оказаться перегруженным, что приведет к задержкам в проведении процедуры аутентификации, а в отдельных случаях даже к отказам в аутентификации легальных

пользователей. Таким образом, особенно актуальными являются вопросы повышения эффективности использования каналов связи в КС при заданном уровне защищенности обрабатываемой информации.

В современных корпоративных КС узлы (рабочие станции — РС) распределены на значительной территории и для передачи информации в них чаще всего используется протокол TCP/IP. Реализация средств защиты информации, в частности механизмов аутентификации в данных сетях, обусловливает увеличение объема передаваемой информации, что ввиду использования относительно медленных, в том числе коммутируемых каналов связи и значительного количества пользователей сети (число которых достигает 1000 и более), может привести к перегрузкам сетевых каналов связи.

Таким образом, весьма актуальной является разработка специальных средств управления передачей данных в защищенных КС на основе протокола TCP/IP, реализующих предотвращение возможных перегрузок в сети и эффективное распределение пропускной способности сетевых каналов связи между пользователями.

1. ПРОБЛЕМА ПЕРЕГРУЗОК В КОМПЬЮТЕРНЫХ СЕТЯХ НА ОСНОВЕ ПРОТОКОЛА TCP/IP

Под перегрузкой компьютерной сети понимается такое ее состояние, при котором сетевые ресурсы на протяжении достаточно длительного интервала времени не способны обрабатывать поступающие задания [3]. В компьютерных сетях на основе протокола TCP/IP перегрузки возникают из-за отсутствия централизованного управления сетевыми ресурсами. Например, когда в маршрутизатор или сервер поступает одновременно несколько TCP–пакетов, которые должны быть отправлены на один адрес, либо на один маршрутизатор (сервер) за короткий интервал времени приходит множество пакетов от различных отправителей. Поскольку пакеты могут быть обработаны лишь последовательно, в случае одновременного поступления нескольких пакетов необходимо применение специального механизма, определяющего порядок их обработки и передачи (пакеты, ожидающие обработки, могут помещаться в специальную буферную память маршрутизатора (сервера) и далее обрабатываться в соответствии с дисциплиной FIFO).

Применение механизма буферной памяти в сетевых маршрутизаторах и серверах позволяет обрабатывать весь сетевой трафик при незначительном увеличении его интенсивности. Однако, если интенсивность передачи пакетов существенно возрастает, то с учетом конечного размера буферной памяти пакеты будут теряться.

Проблема перегрузки не может быть разрешена реализацией принципа неограниченной буферной памяти, поскольку в этом случае также неограниченно возрастает длина очереди пакетов, и, как следствие, неограниченно увеличиваются задержки передачи пакетов от отправителей к полу-

чателям. Кроме того, время, выделяемое на обработку одного пакета в КС, часто ограничено, и при перегрузке сети часть пакетов будет потеряна, что потребует их повторной передачи [4]. Таким образом, существенное увеличение размера буферной памяти в маршрутизаторах и серверах является неэффективным, так как в этом случае часть пакетов будет потеряна уже после того, как они достаточно длительное время занимали сетевые ресурсы.

К перегрузкам в компьютерных сетях могут приводить следующие ситуации [3]:

1) существенное увеличение объема передачи данных по одному сетевому каналу (часто ввиду одновременной работы нескольких пользователей);

2) TCP-протокол повторно передает пакеты, которые уже находятся в процессе передачи или даже приняты получателем (что возможно, если время передачи превышает некоторое критическое значение), при этом увеличение физической пропускной способности каналов связи является лишь временным решением данной проблемы;

3) потеряны пакеты, которые некоторое время передавались по сети, но не были доставлены получателю, сетевые ресурсы были заняты данными пакетами фактически впустую;

4) фрагментация пакетов, когда в сети передаются фрагменты, которые будут в дальнейшем удалены, так как из них невозможно восстановить исходный пакет.

Результатом перегрузок в компьютерной сети является высокий уровень потери пакетов, существенное увеличение времени их доставки от отправителя к получателю и даже временная недоступность сетевых ресурсов и сервисов. Перегрузка в КС при выполнении процедуры аутентификации может привести к невозможности реализации данных средств защиты информации.

Таким образом, весьма актуальной является разработка и применение средств управления сетевым трафиком, которые позволят избежать потенциальных перегрузок в КС. В настоящее время с этой целью разработаны средства, получившие название «механизмы управления перегрузкой в компьютерных сетях».

2. МЕХАНИЗМЫ УПРАВЛЕНИЯ ПЕРЕГРУЗКОЙ В КОМПЬЮТЕРНЫХ СЕТЯХ

Существует два основных класса механизмов управления перегрузкой в компьютерных сетях: 1 — механизмы, реализуемые на узлах (PC) сети и 2 — на маршрутизаторах или серверах (рис. 1). Механизмы первого класса выполняют управление исходящим, а второго — входящим сетевым трафиками. Рассмотрим особенности реализации приведенных на рис. 1 средств управления перегрузкой в КС.

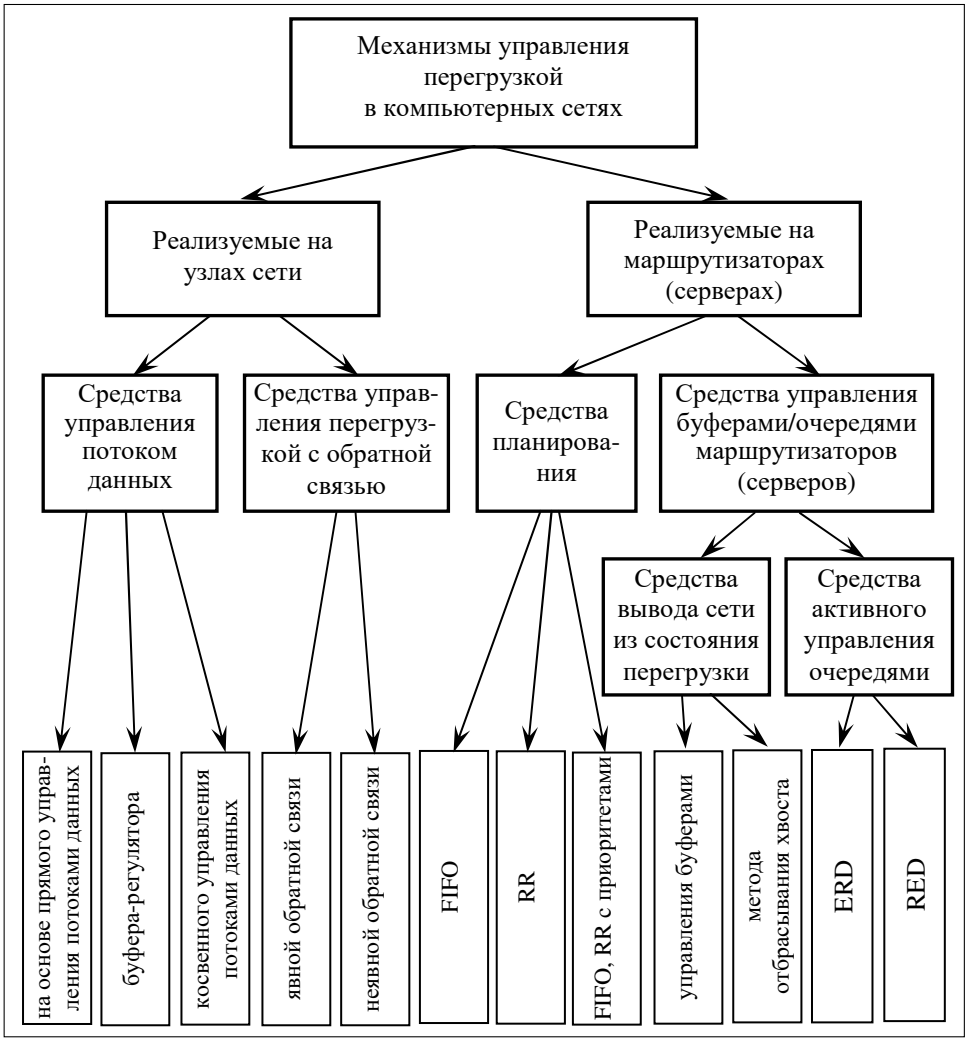

Рис. 1. Классификация механизмов управления перегрузками в КС

3. МЕХАНИЗМЫ УПРАВЛЕНИЯ ПЕРЕГРУЗКОЙ КОМПЬЮТЕРНОЙ СЕТИ, РЕАЛИЗУЕМЫЕ НА ЕЕ УЗЛАХ

3.1. Средства управления перегрузкой КС на основе управления потоками данных между узлами сети

Существует два подхода к реализации средств данного типа: метод прямого и метод косвенного управления потоками данных.

Средства управления перегрузкой КС на основе прямого управления потоками данных реализуются в тех сетях, где взаимное влияние пользователей не учитывается или является незначительным. В данном случае отправитель устанавливает необходимую ему пропускную способность сети, определяя максимальную длину очереди пакетов и интервалы времени между поступлениями пакетов. Средства управления сетью проверяют значения установленных пользователем параметров, и если они являются допустимыми, то для данного пользователя выделяются соответствующие сетевые

ресурсы и маршрут следования пакетов. В процессе передачи пакетов отправитель должен убедиться в том, что обеспечивается установленная им пропускная способность, и перегрузок в сети нет. Следует отметить, что данный подход не может быть реализован средствами лишь одного узла и требует распределенного управления ресурсами.

Одной из проблем реализации данных средств является необходимость формального описания поведения отправителей на основе ограниченного числа параметров. Предварительное резервирование сетевых ресурсов может привести к снижению пропускной способности сети из-за того, что отправители посылают пакеты с различной интенсивностью и могут ограничивать время их обработки в сети. Для задания пропускной способности сети целесообразно определить функцию интенсивности поступления пакетов, устанавливающую число передаваемых пакетов за фиксированный интервал времени.

Еще один из вариантов реализации метода прямого управления потоками данных — использование буфера-регулятора, управляющего длиной очереди пакетов в соответствии с заданной функцией интенсивности поступления пакетов. В данном случае пакеты накапливаются в буферной памяти и отсылаются лишь тогда, когда накоплено определенное число пакетов.

Средства управления перегрузкой КС на основе косвенного управления потоками данных реализуются в компьютерных сетях с динамической реконфигурацией, в которых пропускная способность варьируется с целью эффективного использования сетевых ресурсов. В этих средствах используется принцип адаптивного окна, реализующий управление пропускной способностью КС путем изменения числа отправленных, но не подтвержденных пакетов, или принцип адаптивной пропускной способности, когда при отправлении нового пакета запускается таймер со значением, обратно пропорциональным значению требуемой пропускной способности, причем следующий пакет передается лишь после окончания промежутка времени, определенного таймером. Подход на базе адаптивного окна более прост в реализации, так как он не требует использования точного таймера, достаточно трудно реализуемого в обычных операционных системах. Следует отметить, что при определенных условиях принцип косвенного управления потоком данных может вызвать потерю большого числа пакетов или снизить эффективность использования сетевых ресурсов.

3.2. Средства управления перегрузкой КС с обратной связью

В средствах такого типа используется принцип уведомления отправителя о текущей пропускной способности сети и о сетевых перегрузках. В этом случае активное участие принимают серверы, маршрутизаторы и узлы получателей, посылающие отправителям сигналы о перегрузке в КС по обратной связи. Отправитель может получать информацию двумя путями: либо непосредственно от сетевых ресурсов, либо от получателя. Существует два вида таких средств управления перегрузкой КС: с неявной и явной обратной связью.

3.2.1. Средства управления перегрузкой КС с неявной обратной связью

В данных средствах узлы сети выполняют анализ величин задержки передачи пакетов и числа потерянных пакетов. Эти средства также могут реализоваться на основе анализа зависимости задержек передачи пакетов от уровня

пропускной способности сети. При этом потеря пакетов не может служить однозначным индикатором перегрузки, так как потеря большого числа пакетов характерна, например, для мобильных сетей. Для устранения перегрузок в данных средствах используется метод принудительного удаления пакетов.

Преимущество средств с неявной обратной связью — простота их реализации на маршрутизаторах, которые при этом выполняют лишь свои прямые функции и не генерируют сигналов обратной связи. Однако для эффективной реализации данных средств необходимо использование механизмов планирования передачи пакетов маршрутизаторами, иначе полученные характеристики пропускной способности и индикация ситуаций перегрузки КС могут оказаться некорректными.

3.2.2. Средства управления перегрузкой КС с явной обратной связью

В таких средствах сигналы о перегрузках в сети генерируются непосредственно на основе анализа пропускной способности КС. Ввиду того, что сигналы о перегрузках в КС размещаются в заголовках пакетов, а размер заголовков ограничен, то эти сигналы являются битовыми (0/1) или занимают 2–3 бита. Известны два основных вида таких средств управления перегрузкой: путем управления интенсивностью передачи пакетов отправителем и на основе явной индикации перегрузки.

В средствах первого вида сигнал о необходимости снижения интенсивности передачи пакетов отсылается отправителю в том случае, если в узле или маршрутизаторе (сервере) были потеряны пакеты или их буферная память переполнена.

В средствах на основе явной индикации перегрузки в случае перегрузки в сети маршрутизатор устанавливает в 1 бит CE в заголовке пакета, после чего в узле получателя данный бит копируется в заголовок пакета подтверждения, и далее по определенному алгоритму изменяется размер TCP-окна, т.е., фактически, пропускная способность сети.

Ввиду того что передача сигналов обратной связи снижает общую пропускную способность канала связи, данные средства не обладают повышенной эффективностью для предотвращения перегрузок в сети, но, с другой стороны, позволяют достаточно точно оценить состояние трафика КС, что весьма важно в практических приложениях [5].

4. МЕХАНИЗМЫ УПРАВЛЕНИЯ ПЕРЕГРУЗКОЙ В КОМПЬЮТЕРНЫХ СЕТЯХ, РЕАЛИЗУЕМЫЕ НА МАРШРУТИЗАТОРАХ (СЕРВЕРАХ)

4.1. Средства управления перегрузкой КС на основе планирования обслуживания пакетов

Такие средства реализуют определенную дисциплину обслуживания пакетов и таким образом выполняют непосредственное управление процессом прохождения пакетов по сети. Тип дисциплины обслуживания пакетов определяет распределение пропускной способности канала между пользователями, так как в зависимости от типа дисциплины за фиксированный интервал времени будет обслужено определенное число пакетов конкретного отправителя.

При выборе типа дисциплины обслуживания пакетов учитываются следующие факторы: принципы выборки пакетов из очереди и обслуживания пакетов с одним уровнем приоритета, число уровней приоритетов для обработки пакетов.

Различают активную и пассивную выборки пакетов из очереди. При активной выборке пакеты не извлекаются из очереди лишь в том случае, если она пуста. При пассивной пакеты не извлекаются из очереди до тех пор, пока не будут выполняться некоторые заранее определенные условия. В качестве таких условий могут выступать, например, значения интенсивности поступления пакетов или длина очереди пакетов.

Принцип обслуживания пакетов с одним уровнем приоритета — один из основных элементов управления передачей данных и играет ключевую роль при реализации TCP/IP-протокола. Поступающие пакеты должны обрабатываться оптимальным образом для обеспечения требуемой скорости передачи пакетов в сети.

Простейший принцип обслуживания пакетов — FIFO: пакеты обслуживаются в порядке их поступления, при этом все пакеты находятся в очереди приблизительно одинаковое время. Принцип FIFO не обеспечивает адаптивного обслуживания пакетов, поскольку он не учитывает их специфику.

Более сложный принцип обслуживания пакетов — дисциплина RR (Round-robin): маршрутизатору (серверу) выделяется определенный квант (интервал) времени на обслуживание одного пакета. Если пакет (серия пакетов) имеет длину, большую, чем выделенный квант времени, то он возвращается в очередь и будет обслужен в течение кванта времени в следующем цикле. При этом очередь пакетов обслуживается по принципу FIFO. Спецификой дисциплины обслуживания RR является то, что она позволяет быстро обслужить короткие пакеты.

Разновидность дисциплины RR — вариант ее реализации с несколькими очередями. В этом случае все пакеты изначально поступают в первую очередь. Если кванта времени маршрутизатора (сервера) для обработки пакета недостаточно, он помещается во вторую очередь и далее ожидает своей обработки. Пакеты из q-й очереди могут выбираться лишь в том случае, если все предыдущие $q-1$ очереди пусты. Реализация данной дисциплины позволяет задержать обработку достаточно длинных пакетов (серий пакетов), которые способны на продолжительное время захватить сетевые ресурсы.

В том случае, если в компьютерной сети представлены такие пользователи, которым необходимо дать возможность внеочередного обслуживания данных, например, содержащих аварийную информацию, то вводится принцип приоритетов обслуживания. Каждому пакету приписывается определенное целое число, соответствующее его приоритету, далее очередь сортируется в соответствии с уровнями приоритетов находящихся в ней пакетов. Таким образом, выделяются следующие основные дисциплины приоритетного обслуживания пакетов: FIFO с приоритетами, RR с приоритетами, RR с несколькими очередями и приоритетами.

4.2. Средства управления перегрузкой КС на основе методов обработки буферов и очередей маршрутизаторов (серверов)

Средства управления перегрузкой на основе планирования обслуживания пакетов не могут обеспечить эффективное управление перегрузкой КС. Раз-

мер буферов пакетов в маршрутизаторах (серверах) ограничен, и при высокой интенсивности поступления пакетов на протяжении длительного промежутка времени буферная память будет переполнена, в результате чего число потерянных пакетов в сети может быть значительным.

Таким образом, в КС необходимо использовать специальные методы и средства обработки буферов и очередей пакетов в маршрутизаторах (серверах).

4.2.1. Средства управления буферами пакетов в маршрутизаторах (серверах)

Основной целью средств управления буферами пакетов для предотвращения перегрузок КС является распределение буферной памяти маршрутизатора (сервера) между различными потоками пакетов данных, проходящих через него. Существуют методы статического и динамического распределения буферной памяти, причем выбор конкретного метода определяется количеством потоков пакетов в сети и интенсивностью их поступления. К двум наиболее распространенным методам относятся: случайное распределение буферной памяти между потоками пакетов и распределение с учетом их характеристик. Существуют также и более сложные методы распределения буферной памяти, учитывающие характеристики маршрутизаторов (серверов).

При случайном распределении буферной памяти маршрутизатора (сервера) пакеты обрабатываются в соответствии с принципом FIFO и возможны случаи, когда один поток пакетов занимает всю доступную буферную память, заблокировав обработку всех остальных потоков. Однако из-за простоты данный подход достаточно часто применяется в компьютерных сетях, в частности, в Internet.

В методе распределения буферной памяти маршрутизатора (сервера) с учетом характеристик потоков пакетов последние не могут захватывать всю доступную буферную память и блокировать друг друга. В этом методе выполняется анализ объема буферной памяти, занимаемого различными потоками, и на его основе осуществляется удаление пакетов, принадлежащих определенным потокам. Однако следует отметить, что данный подход достаточно сложен для реализации в маршрутизаторах (серверах), обрабатывающих большие потоки данных.

Увеличение объема буферной памяти пакетов позволяет обслуживать более длинные наборы пакетов без их потерь, однако в результате увеличиваются задержки передачи данных и снижается пропускная способность сети. В практических приложениях в маршрутизаторах (серверах) чаще всего используется буферная память малого объема, что обеспечивает высокую пропускную способность сети.

4.2.2. Средства управления очередями пакетов в маршрутизаторах (серверах)

Основная задача этих средств — управление длиной очереди поступающих пакетов и удаление пакетов по определенным правилам [6]. Средства управления очередями являются, по сути, развитием средств управления перегрузкой на основе планирования и управления буферной памятью маршрутизаторов (серверов). В тех ситуациях, когда интенсивность поступления

пакетов превышает максимально возможную при заданной пропускной способности канала, и при этом действия отправителей по предотвращению перегрузок централизованно не координируются, средства управления очередями пакетов обеспечивают более эффективное управление передачей данных в КС, чем средства планирования обработки пакетов [7].

Существует два основных типа средств управления очередями пакетов в маршрутизаторах (серверах): вывод сети из состояния перегрузки и предотвращение перегрузок КС. Рассмотрим их детальнее.

4.2.3. Средства управления очередями для вывода КС из состояния перегрузки

В простейшем средстве управления очередями в маршрутизаторах (серверах) устанавливается максимально возможная длина очереди, и пакеты принимаются до тех пор, пока она не будет заполнена. Пакеты, приходящие после заполнения, будут теряться до освобождения места в очереди. Потерянные пакеты должны быть переданы по каналам связи повторно.

Данный подход получил название «метод отбрасывания хвоста» и часто применяется в сети Internet, однако имеет существенный недостаток — он не содержит средств обработки заполненной очереди, и потому в сети может возникнуть блокировка передачи всех потоков данных [7]. Это объясняется тем, что факт перегрузки в сети устанавливается лишь тогда, когда очередь уже заполнена. Пакеты в очереди могут оставаться без обработки достаточно длительное время. Кроме того, реализация данного метода может вызвать проблему глобальной синхронизации в сети: при заполнении очереди значительное число пакетов различных отправителей теряется, в результате одновременно снижается интенсивность отправления пакетов, а также эффективность использования канала связи (может возникать пустая очередь пакетов).

Альтернативным подходом к управлению очередями пакетов в маршрутизаторах (серверах) является метод удаления пакетов с начала заполненной очереди при поступлении нового пакета. Этот метод позволяет повысить пропускную способность TCP-протокола, так как, в отличие от метода отбрасывания хвоста, сигнал о перегрузке сети передается отправителю до обработки и передачи всей очереди пакетов, что способствует предотвращению блокировки потоков пакетов [8].

Проблемы глобальной синхронизации и блокировки потоков пакетов могут быть разрешены путем случайной выборки пакетов из очереди [9]. Такие средства реализуются на основе метода случайного удаления пакетов, в котором при поступлении нового пакета в заполненную очередь маршрутизатор (сервер) случайным образом выбирает из очереди пакет для удаления. Важная задача средств управления очередями данного типа — выявление отправителей с высокой интенсивностью передачи пакетов, действия которых представляются возможной причиной перегрузки сети. При этом пакет, который абсолютно случайно выбран из сетевого трафика, принадлежит потоку данных определенного отправителя с вероятностью, пропорциональной скорости передачи его потока данных через маршрутизатор. Однако реализация данных средств управления очередями в маршрутизаторах (серверах) в некоторых случаях достаточно сложная.

4.2.4. Средства предотвращения перегрузок КС на основе методов активного управления очередями

Средства управления очередями в маршрутизаторах (серверах) на основе метода случайного удаления пакетов исключают взаимное блокирование потоков пакетов, но не решают проблему обработки заполненных очередей. Кроме того, во всех представленных выше средствах управления очередями в маршрутизаторах (серверах) отсутствует возможность прогнозирования потенциальных перегрузок в сети до их появления. Таким образом, данные средства выполняют лишь вывод сети из состояния перегрузки и не обеспечивают упреждающее предотвращение перегрузок [7,10].

Эффективная обработка очередей пакетов в маршрутизаторах (серверах) возможна лишь в том случае, если средства управления перегрузкой КС выполняют упреждающие действия до наступления перегрузки, для чего используются методы активного управления очередями. Разработаны методы предотвращения перегрузок, выполняющие по специальному алгоритму удаление определенных пакетов при прогнозировании перегрузки. Удаленные пакеты должны быть повторно переданы по сетевым каналам связи. В этих методах также может выполняться не удаление пакетов (как один из простейших способов борьбы с перегрузкой), а лишь их маркировка некоторым признаком, после чего отправителю передается сигнал о необходимости снижения интенсивности отправления пакетов. Маркировка пакетов заключается в установке определенного бита в заголовке пакета или в другом методе, допустимом для протокола TCP/IP.

Основная цель средств активного управления очередями в маршрутизаторах (серверах) — предотвращение перегрузок сети. При этом решаются и сопутствующие задачи: предотвращение глобальной синхронизации действий отправителей, оптимизация размеров очередей в маршрутизаторах (серверах), предотвращение монопольного захвата сетевого трафика одним потоком данных, снижение числа потерянных пакетов, минимизация задержек при передаче пакетов по сети.

Механизм активного случайного удаления пакетов, являющийся фактически средством вывода сети из состояния перегрузок, также используется для предотвращения перегрузок КС. Данный механизм (ERD — Early Random Drop), получивший название «метод раннего случайного удаления пакетов», предусматривает удаление пакетов еще до заполнения очереди в случае прогнозирования возможной перегрузки. Суть его заключается в том, что число потерянных пакетов (т.е. интенсивность, с которой случайно выбранные пакеты удаляются) зависит от степени перегрузки маршрутизатора (сервера), которая определяется числом пришедших пакетов в интервале между двумя последовательными событиями потери пакетов. Предусматривается фиксированная длина очереди пакетов, однако существуют и более гибкие подходы к определению длины очереди, например, на основе анализа пропускной способности сетевого канала связи.

Средства управления очередями на основе метода ERD более эффективны по сравнению со средствами на основе метода отбрасывания хвоста, поскольку они обеспечивают взаимную изоляцию потоков пакетов, но, с другой стороны, не позволяют оптимальным образом распределять пропускную способность канала между потоками пакетов и эффективно обслуживать потоки данных с высокой интенсивностью.

Для устранения перечисленных выше недостатков средств на основе метода ERD предложен новый метод управления очередями пакетов в маршрутизаторах (серверах) на основе случайного раннего обнаружения (RED — Random Early Detection) [11]. Метод реализуется следующим образом: маршрутизатор (сервер) выявляет возникающие перегрузки в сети путем вычисления среднего размера своей очереди, т.е. в том случае, когда средний размер очереди превышает установленное значение, приходящие пакеты удаляются или маркируются с определенной вероятностью, зависящей от величины превышения средней длины очереди пакетов. В данном методе средняя длина очереди пакетов оказывается достаточно малой, однако при определенных условиях даже длинные серии пакетов могут быть обработаны без потерь. При возникновении перегрузки в сети вероятность удаления (маркировки) пакета из определенного потока данных пропорциональна пропускной способности канала связи, выделенной для этого потока данных.

Существует два подхода к реализации метода RED: на основе анализа средней длины очереди маршрутизатора (сервера) и частоты удаления (маркировки) предыдущих пакетов.

Метод RED адаптируем для управления сетевым трафиком в различных условиях. Однако при определенных параметрах компьютерной сети и сетевого трафика эффективность средств управления очередями маршрутизаторов (серверов) на основе этого метода может приближаться к эффективности аналогичных средств на основе метода отбрасывания хвоста.

5. МЕТОД РАННЕГО ПРИОСТАНОВЛЕНИЯ ПЕРЕДАЧИ ПАКЕТОВ ДЛЯ ПРЕДОТВРАЩЕНИЯ ПЕРЕГРУЗОК В КОМПЬЮТЕРНЫХ СЕТЯХ

Как уже упоминалось выше, одной из главных проблем средств управления передачей данных в КС на основе активного управления очередями является то, что удаленные пакеты должны быть повторно переданы по сетевому каналу связи. Таким образом, возрастают затраты времени на обработку этих пакетов, а также возникает проблема неэффективного использования сетевых ресурсов (пакет передавался по сети, находился некоторое время в очереди маршрутизатора (сервера), но затем был удален).

Предлагается новый метод раннего приостановления передачи пакетов (РППП) на основе принципа активного управления очередями, который позволяет практически избежать процедуры удаления пакетов, что обеспечивает повышенную эффективность его применения.

Рассмотрим суть предлагаемого метода. На рис. 2 изображен фрагмент КС, состоящий из маршрутизатора (сервера), обслуживающего пакеты, поступающие от РС (узлов).

Специфика предлагаемого метода состоит в том, что он предусматривает управление не только входящим трафиком (в маршрутизатор или сервер), но также и исходящим трафиком от РС, что позволяет гибко изменять интенсивность отправления пакетов (и, как результат, скорость заполнения очереди пакетов на маршрутизаторе (сервере)) и избежать удаления пакетов.

На первом этапе реализации метода РППП все потоки пакетов поступают в очередь маршрутизатора (сервера) до ее заполнения. После того как

очередь маршрутизатора (сервера) оказывается заполненной, всем РС отсылается сигнал на запрет передачи пакетов, и генерируемые ими пакеты помещаются в буферную память пакетов РС. После того как очередь маршрутизатора (сервера) освободится на количество пакетов, соответствующее числу активных пользователей сети (РС), от каждой РС на маршрутизатор (сервер) будет передано по одному пакету. Если буферы пакетов всех РС были заполнены, то, соответственно, и очередь маршрутизатора (сервера) заполнится вновь. Далее РС снова будет послан сигнал о занятости очереди маршрутизатора (сервера) и процедура передачи пакетов от РС повторится. На данном этапе реализуется режим передачи данных по одному пакету от каждого источника. Как только поток пакетов хотя бы от одного источника прекратится, в очереди появится свободное место, и пакеты от РС будут передаваться в обычном режиме до получения нового сигнала о заполнении очереди.

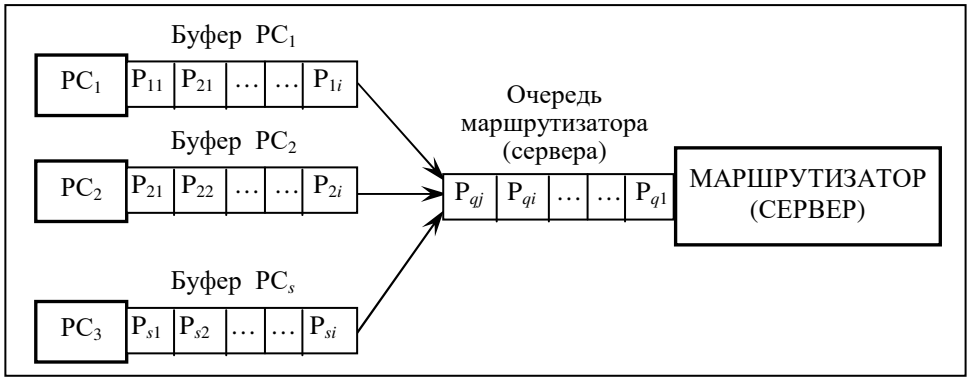

Рис. 2. Передача пакетов в фрагменте КС из s рабочих станций (РС) и маршрутизатора (сервера)

Преимуществом предлагаемого метода РППП является отсутствие удаленных пакетов. Ни один пакет не будет передан повторно из-за действий средств управления передачей данных.

Рассмотрим аналитические модели одного цикла работы метода RED и предлагаемого метода РППП.

Обозначим:

t_1 — среднее время передачи пакета от отправителей (РС) к маршрутизатору (серверу); t_2 — среднее время пребывания пакета в очереди маршрутизатора (сервера); N — общее число сгенерированных и переданных пакетов; p — число потерянных пакетов (для метода RED); p' — число приостановленных пакетов (для метода РППП).

Пропускная способность маршрутизатора (сервера) рассчитывается по формуле

$$\gamma = \frac{L_p}{T}, \qquad (1)$$

где $L_p = N * l$ — суммарная длина всех обработанных пакетов; l — длина одного пакета (условимся, что все пакеты имеют одинаковую длину); T — суммарное время передачи N пакетов по каналу связи и пребывания их в очереди маршрутизатора (сервера).

Для средств управления передачей данных на основе метода RED параметр T равен

$$T_{\text{RED}} = N*t_1 + (N-p)*t_2 + p*t_1 + p*t_2 = N*(t_1+t_2) + p*t_1, \qquad (2)$$

причем $(N-p)$ — длина очереди пакетов.

Для средств управления передачей данных на основе предлагаемого метода РПППП параметр T определяется как

$$T_{\text{РПППП}} = (N-p')*t_1 + (N-p')*t_2 + p'*t_1 + p'*t_2 + p'*t_2 =$$

$$= N*(t_1+t_2) + p'*t_2. \qquad (3)$$

Дополнительный член $p'*t_2$ появляется вследствие того, что приостановленные пакеты ожидают освобождения очереди маршрутизатора (сервера).

Поскольку в предлагаемом методе РПППП приостановленные пакеты фактически соответствуют удаленным в методе RED, то принимаем $p = p'$.

Пропускная способность канала связи маршрутизатора (сервера) рассчитывается таким образом:

для средств на основе метода RED

$$\gamma_{\text{RED}} = \frac{N*l}{N(t_1+t_2) + p*t_1}, \qquad (4)$$

для средств на основе предлагаемого метода РПППП

$$\gamma_{\text{РПППП}} = \frac{N*l}{N(t_1+t_2) + p*t_2}. \qquad (5)$$

Из соотношений (4) и (5) видно, что если $t_1 > t_2$, т.е. время передачи одного пакета по сетевым каналам связи больше, чем время его обработки в очереди маршрутизатора (сервера), как часто бывает в практических приложениях, то предлагаемый метод РПППП для управления очередями обеспечивает более высокую пропускную способность передачи пакетов по сети.

Известно, что в защищенных КС часто обрабатывается информация различной степени секретности (защищенности). Информация с более высокой степенью защищенности обычно является приоритетной и ее необходимо обработать в первую очередь. Пользователям защищенных КС присваиваются ранги в соответствии с уровнем секретности информации, которую они обрабатывают и передают.

Таким образом, возникает задача гибкого управления пропускной способностью каналов связи маршрутизаторов (серверов) с предоставлением приоритетов (т.е. ускоренной передачи пакетов) пользователям, обрабатывающим информацию с высоким рангом секретности.

Некоторая модификация предложенного метода РПППП позволяет решить эту задачу. Рассмотрим для примера случай, когда выделяются пользователи только двух рангов — высокого и низкого (ситуации, когда в КС присутствуют пользователи с большим числом рангов также возможны, но они требуют дополнительной модификации метода с учетом всего количества рангов). В этом случае после первичного заполнения очереди маршрути-

затора (сервера) на втором этапе блокируются все потоки пакетов, кроме того, который генерируется пользователем с высоким рангом. В сети может быть одновременно несколько пользователей с высоким рангом, и сетевой канал связи будет разделен только между ними.

Пропускная способность маршрутизатора (сервера) для данных пользователей при использовании модифицированного метода РППП (мод РППП)

$$\gamma_{\text{мод РППП}} = \frac{N * l}{N(t_1 + t_2) + n * t_2}, \qquad (6)$$

где n — количество пользователей с высоким рангом секретности.

Если $n < p = p'$, то пропускная способность маршрутизатора (сервера) для пользователей с высоким рангом будет повышена по сравнению с его пропускной способностью для случая, когда все пользователи имеют одинаковый ранг, что позволяет адаптивно обслужить приоритетных пользователей.

На рис. 3 показана зависимость пропускной способности маршрутизатора (сервера) γ (Кбайт/с) от коэффициента k ($k = t_1 / t_2$), отражающего соотношение между средним временем передачи одного пакета и средним временем его пребывания в очереди, для метода RED, предложенного метода РППП для пользователей одного ранга, модифицированного метода РППП при одном ($n = 1$) высокоранговом пользователе и модифицированного метода РППП при пяти ($n = 5$) высокоранговых пользователях. При этом для расчетов использовались следующие значения параметров: число передаваемых пакетов $N = 1000$, длина пакета (усредненно) $l = 50$ байт, среднее время пребывания пакета в очереди маршрутизатора (сервера) $t_2 = 1$с, число потерянных (приостановленных) пакетов $p = 250$.

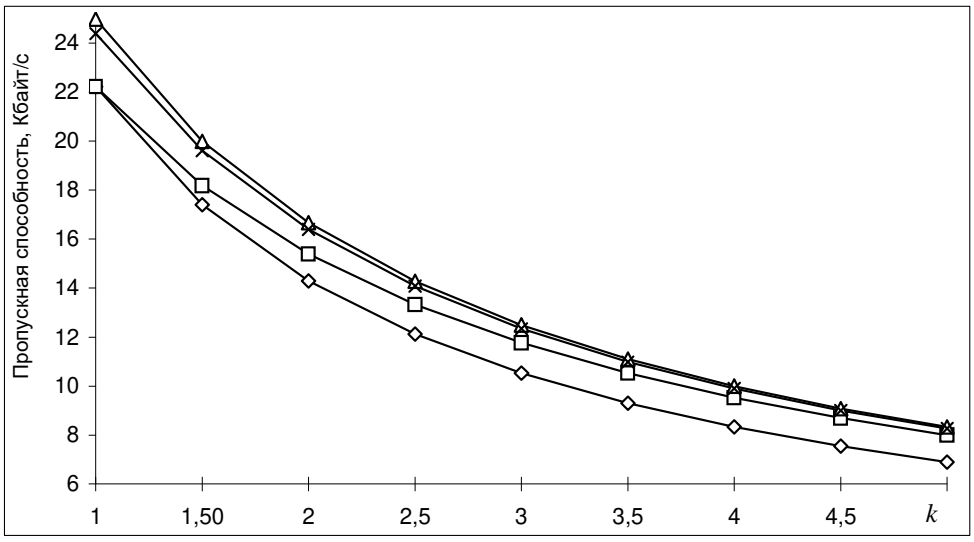

Рис. 3. Зависимость пропускной способности маршрутизатора (сервера) γ от коэффициента k ($k = t_1 / t_2$) для различных методов предотвращения перегрузок в сети: ◇ — алгоритм RED; □ — алгоритм РППП; Δ — модифицированный алгоритм РППП при одном высокоранговом пользователе; × — модифицированный алгоритм РППП при пяти высокоранговых пользователях

Как видно из рис. 3, применение предложенного метода РППП для предотвращения перегрузок сети позволяет повысить пропускную способ-

ность маршрутизатора (сервера) в зависимости от значения коэффициента k на $10-16\%$. Для модифицированных методов РППП, применяемых в случае ранжирования пользователей КС в соответствии с уровнем секретности передаваемых ими данных, рост пропускной способности оказывается еще выше и достигает $15-20\%$.

Таким образом, проведенные исследования моделей средств предотвращения перегрузок в КС на основе методов активного управления очередями пакетов подтверждают повышенную эффективность предлагаемых методов по сравнению с распространенным методом RED.

ЗАКЛЮЧЕНИЕ

Вопросы эффективного управления передачей данных в компьютерных сетях, реализующих средства защиты обрабатываемой информации, весьма актуальны. Применение средств защиты снижает пропускную способность пользовательской информации в компьютерных сетях, так как эти средства осуществляют передачу дополнительных служебных данных по сети. Кроме того, в результате использования механизмов защиты информации увеличивается объем данных, передаваемых по сети, что при определенных условиях может привести к перегрузкам сетевых каналов связи.

Предлагаемые в статье методы и средства предотвращения перегрузок в сетях на основе активного управления очередями пакетов в маршрутизаторах (серверах) обеспечивают гибкое управление передачей данных в защищенных компьютерных сетях, что особенно важно в практических приложениях для повышения эффективности реализации различных сетевых сервисов.

ЛИТЕРАТУРА

1. *Олифер В.Г., Олифер Н.А.* Компьютерные сети. Принципы, технологии, протоколы. — СПб.: Питер, 2002. — 672 с.
2. *Широчин В.П., Мухин В.Е.* Формализация и целевая адаптация средств аутентификации в компьютерных сетях // УС и М. — 2000. — № 5/6. — С. 59–65.
3. *Congestion* Control Mechanisms and Best Effort Service Model / P. Gevros, J Crowcroft, P. Kirstein, S. Bhatti // IEEE Network, May/June 2001. — P. 16–26.
4. *Mathis M.* et al. The Macroscopic Behavior of the TCP Congestion Avoidance Algorithm // Computer Communication Review, July 1997. — P. 73 – 81.
5. *Ramakrishnan K., Floyd S.* A Proposal to Add Explicit Congestion Notification (ECN) to IP. RFC 2481, IETF, Jan 1999. — 34 p.
6. *Firoiu V., Barden M.* Queue Management for Congestion Control // Proc. IEEE INFOCOM, San Francisco, USA, May 2000. — P. 136 –150.
7. *Suter B.* Efficient Active Queue Management for Internet Routers // Proc. of Intern. Conference Interop'98, Las Vegas, USA, May 1998. — P. 144 –147.
8. *Lakshman T.V., Neidhardt A., Ott T.J.* Drop from Front Strategy in TCP and in TCP over ATM // Proc. IEEE INFOCOM, San Francisco, USA, March 1996. — P. 101–113.
9. *Floyd S., Fall K.* Promoting the Use of End-to-End Congestion Control in the Internet. IEEE ACM Trans. on Networks, Aug. 1999. — P. 58–67.
10. *Morris R.* Scalable TCP Congestion Control // Proc. IEEE INFOCOM, San Francisco, USA, May 2000. — P. 258–271.
11. *Floyd S., Jacobson V.* Random Early Detection Gateways for Congestion Avoidance. IEEE/ACM Trans. on Networks. — **1**, № 4. — Aug. 1996. — P. 26 – 42.

Поступила 02.12.2004