Р. Н. Залата

АГРЕГАЦИЯ И СТАТИСТИЧЕСКАЯ ПРЕДОБРАБОТКА АККАУНТИНГОВОЙ ИНФОРМАЦИИ С ЦЕЛЬЮ ОПТИМИЗАЦИИ ОПЕРАЦИЙ С СУБД ДЛЯ СИСТЕМ УЧЕТА И МОНИТОРИНГА КОРПОРАТИВНЫХ СЕТЕЙ

В процессе разработки систем мониторинга и расчета трафика для корпоративных сетей встает вопрос большого объема хранимых и обрабатываемых данных (аккаунтинговой информации), что ведет к чрезмерно завышенному потреблению вычислительных ресурсов такими системами. В статье приведены алгоритмы статистической предобработки аккаунтинговой информации, за счет которых достигается значительная экономия ресурса СУБД и увеличение производительности операций на несколько порядков. Алгоритмы подтверждены экспериментальными данными, результаты которых также приведены в статье.

1. Актуальность проблемы

Для мониторинга, диагностики и тарификации пользователей IP сетей, как корпоративных — интранет, так и публичных — интернет, необходимо иметь механизм фиксирования трафика, создаваемого пользователями и передаваемого ими через сеть [1]. На данный момент широко используются два механизма сбора аккаунтинговой информации (статистической информации о переданных через сеть пользовательских потоках данных, тарификацию или мониторинг которых необходимо осуществлять) с IP сетей, а именно технологии «ip accounting» и «netflow» [2].

Оба этих механизма позволяют периодически получать полную информацию о всех переданных через сеть пользовательских потоках данных в виде таблиц (см. пример на рис. 1). Каждый поток информации представляется в таблицах одной записью, которую принято называть «аккаунтинговой информацией» (от англ. «account» — обсчет) [3]. Обобщенный формат записей для IP трафик описан в [2] и представлен на рис. 1 со следующими информационными полями:

- *«тип протокола»* — определяет тип потока (tcp, udp, icmp или иной);
- *«IP адрес источника»* и *«порт источника»* — определяют источник IP пакетов в данном потоке, а именно адрес в сети и тип серверного приложения, создавшего поток;
- *«IP адрес назначения»* и *«порт назначения»* — определяют адрес пользователя, в сторону которого передаются пакеты потока;
- *«период»* — временные отметки начала и конца моментов времени, за которое собрана информация о данном потоке;
- *«байт передано»* — общая сумма трафика в байтах по данному потоку за указаный период.

Период	*Тип протокола*	*IP адрес источника*	*Порт источника*	*IP адрес назначения*	*Порт назначения*	*Байт передано*

Рис. 1. Обобщенный формат таблицы IP accounting'а или NetFlow потока

Чем больше пользовательских информационных потоков проходит через сеть и чем больше период сбора информации, тем чаще и в большем количестве генерируется информация с активного оборудования сети (маршрутизаторов, коммутаторов и серверов) об этих потоках, тем больше записей содержат таблицы. Данные таблиц сохраняются в СУБД для последующей обработки в системах тарификации, диагностики или мониторинга состояния сети.

В корпоративных сетях, а также на узлах телематических служб, при большом потоке транзитного трафика и необходимости сохранять аккаунтинговую информацию за большой предшествующий моменту тарификации срок (например, за месяц) [3], возникает проблема хранения и оперативного доступа к этой информации через СУБД. По проведенным измерениям на корпоративной сети ТюмГНГУ за месяц работы в СУБД скапливается более 10 миллионов записей аккаунтинговой информации. Расчет трафика по пользователям, проводимый ежемесячно, потребляет много вычислительных ресурсов и занимает по времени более суток. Необходимость сохранения в СУБД аккаунтинговой информации за несколько периодов (3, 6 или 12 месяцев) приводит к тому, что объем потребляемых СУБД ресурсов растет, а производительность (скорость произведения выборки из БД) падает пропорционально количеству хранимых в СУБД записей. Это обстоятельство создает массу трудностей при последующей обработке аккаунтинговой информации или даже делает невозможным выполнение некоторых операций из-за отсутствия должного количества вычислительных ресурсов.

Проблема частично разрешается путем увеличения вычислительной мощности аккаунтинговой системы: оперативной памяти, тактовой частоты и числа вычислительных процессоров. Другой спо-

соб решения проблемы, описанный в [4], состоит в том, чтобы снабжать активные устройства сети (источники аккаунтинговой информации) дополнительными аппаратными средствами по сбору и обработке аккаунтинга. Последний метод эффективен, но дорогостоящ, а его внедрение потребует полной реконфигурации инфраструктуры сети.

Проблему можно решить не прибегая к дополнительным и ощутимым капиталовложениям, а также не производя каких-либо изменений в устройстве сети, путем агрегации и статистического анализа аккаунтинговой информации перед ее сохранением в СУБД. С этой целью автором было предложено несколько не сложных, быстро вычислимых алгоритмов предобработки. Эффективность использования этих алгоритмов была оценена на трех различных сетях с разным контингентом пользователей.

По проведенным экспериментам, применение этих алгоритмов позволяет уменьшить общий объем сохраняемой аккаунтинговой информации в 10 раз и примерно во столько же раз увеличить производительность СУБД при последующей обработке этой информации (т. е. для тарификации, мониторинга и диагностики IP сетей).

2. Агрегация аккаунтинговой информации

Схема информационных потоков в IP сетях такова, что генерируемая с них аккаунтинговая информация (т. е. записи формата, приведенного на рис. 1) имеет регулярную структуру, а именно данные в аккаунтинговых таблицах регулярно повторяются, при этом меняются только временные отметки в полях «*период»* и счетчики в поле «*байт передано»*. Связано это с тем, что пользователи, инициирующие информационные потоки в сети, с одной стороны, используют достаточно ограниченное число сетевых информационных ресурсов (располагающихся на так называемых сайтах), с другой — регулярно обращаются к одним и тем же сайтам сети (корпоративным или в глобальной сети). Так, если не принимать во внимание значения в полях «период» и «байт передано» и предположить, что число пользователей относительно невелико (много меньше числа записей в аккаунтинговых таблицах), число регулярно посещаемых пользователем сайтов также ограничено, то среднее количество уникальных записей за определенный период в таблице аккаунтинга (среднее число уникальных информационных потоков за период) можно оценить по следующей зависимости:

$$N\text{с} = N\text{п. с.} * N\text{р. с.},$$

где *N*п. с. — среднее число пользователей в сети, проявляющих активность в заданный период времени, а *N*р. с. — среднее число сайтов, посещаемых пользователем за указанный период.

По результатам проведенного эксперимента в корпоративной сети ТюмГНГУ, которая насчитывает около 250 пользователей [1], среднее число активных пользователей сети *N*п. с. равно 54. Количество уникальных ресурсов, к которым обращается средний пользователь сети (*N*р. с.), в зависимости от оценочного периода приведено в табл. Среднее значение этого параметра для периода длительностью в 10 часов составляет *N*р. с. = 541 сайт. Тогда среднее количество уникальных информационных потоков, создаваемых пользователями корпоративной сети ТюмГНГУ, составляет *N*с = 541 * 54 = 29 214 за указанный период.

Зависимость среднего числа посещенных уникальных сайтов средним пользователем от длительности анализируемого периода

Время начала периода	Время конца периода	Длительность, ч	Число уникальных сайтов за весь период	Прирост числа уникальных сайтов за 1 ч
9:00	10:00	1	55	55
9:00	11:00	2	120	65
9:00	12:00	3	222	102
9:00	13:00	4	336	114
9:00	14:00	5	411	75
9:00	15:00	6	441	30
9:00	16:00	7	459	18
9:00	17:00	8	514	55
9:00	18:00	9	534	20
9:00	19:00	10	541	7

Рассчитанное в результате эксперимента число записей в таблице аккаунтинга является минимальным, а содержащаяся в ней информация агрегирована по времени (в данном случае за 10 часов). Очевидно, что агрегирование аккаунтинговой информации периодами по 10 часов дает ощутимый выигрыш в экономии числа записей (и как следствие — экономии ресурсов СУБД и увеличении скорости обработки запросов), в несколько сотен раз. Однако агрегирование информации

такими большими периодами делает ее мало приемлемой для дальнейшего использования, так как большая часть полезной информации скрывается агрегацией.

Для того чтобы достичь некоего компромисса между производительностью (и экономией ресурсов) и «полезностью» сохраняемой информации, на практике рекомендуется использовать периоды агрегации не более ½ или 1 часа. В этом случае также достигается значительная экономия ресурса БД и, в то же время, аккаунтинговая информация является достаточно детализированной для последующего применения.

Алгоритм создания таких агрегированных аккаунтинговых таблиц не представляет особой сложности в реализации и легко вычислим. Чтобы агрегировать аккаунтинговую таблицу, необходимо аккумулировать аккаунтинговую информацию в течение определенного времени, суммировать значения счетчиков в полях *«байт передано»* для всех потоков с одинаковыми значениями во всех остальных одноименных полях (т. е. для потоков с одинаковыми идентификаторами источника и назначения). По истечении периода агрегирования получаемые аккумулированные записи сохраняются в БД.

3. Предобработка аккаунтинговой информации

В случае больших объемов собираемой аккаунтинговой информации даже ее агрегирование описанным выше методом может не дать значительного результата оптимизации числа записей в БД. Однако в процессе детального анализа собираемой акаунтинговой информации на корпоративной сети ТюмГНГУ была выявлена следующая закономерность: большая часть записей в таблицах аккаунтинга отражает потоки с относительно небольшими значениями счетчиков переданного трафика.

С учетом этой закономерности на корпоративной сети ТюмГНГУ (а также на нескольких других сетях) был проведен ряд экспериментов. Суть их состояла в том, чтобы просуммировать значения счетчиков передаваемого трафика (за фиксированный период времени) и взвесить их процентные отношения от всего трафика. Результаты измерений оказались следующими: порядка 75 % числа записей о потоках передаваемого трафика в сети отражают не более 5 % объема всего переданного трафика. То есть, если пренебречь этими записями (удалить их из СУБД или не вносить вообще), то реальная погрешность, вносимая в общий трафик, не превысит 5 %.

Таким образом, производя отсечения (удаления) малоинформативных агрегатов (агрегированных записей в таблице аккаунтинга, полученных описанным выше способом) и оценивая вносимую при этом погрешность в вычисления трафика, удерживая ее в определенных рамках, можно сократить расходуемый ресурс БД еще в несколько раз. На рис. 2 приведены два графика: **зависимости экономии объема БД** и **зависимости вносимой погрешности в вычисления** потоков от размера отсекаемого агрегата. Из графика видно, что при отсечении всех агрегатов, счетчик трафика в которых меньше 15 000 байт, вносимая погрешность не превышает 5 % и достигается экономия (и, как следствие, увеличение скорости обработки данных в БД, экономия ресурсов) в 65 % от общего числа записей в таблицах аккаунтинга.

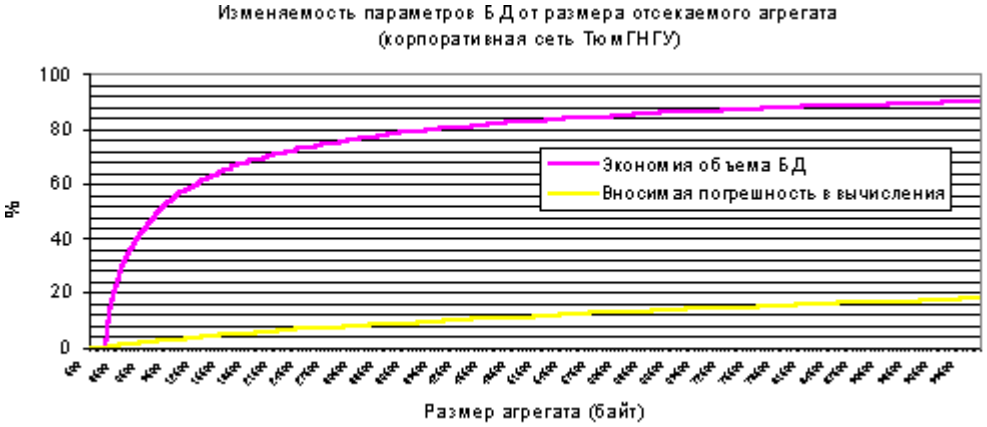

Рис. 2. Зависимость вносимой погрешности
и экономии объема записей в БД от размера отсекаемого агрегата

Процент вносимой погрешности и достигаемый эффект оптимизации, как видно из графиков, зависят от размера отсекаемого агрегата. Не сложно составить простую имитационную модель, динамически пополняя которую эмпирическими данными (непрерывно поступающими в процессе сборки аккаунтинговой информации), можно достигать максимума эффективности и при этом удерживать значение вносимой погрешности в определенных фиксированных пределах (к примеру, точность расчета трафика в процессе тарификации должна быть в пределах +5…-5 %).

Вывод

Используя вышеописанные методы предобработки аккаунтинговой ин-формации, путем агрегации с последующим отсечением малоинформативных агрегатов можно достичь значительной экономии ресурсов СУБД и оптимизации вычислений в процессе последующей обработки собранных данных в сотни раз. Достигаемый таким образом эффект полезен для реализации «real-time» систем мониторинга и тарификации, в которых все процессы происходят в режиме «реального времени» и являются очень критичными к скорости доступа к данным и объему производимых над ними вычислений.

Описанные методы реализованы в разрабатываемой на данный момент системе аккаунтинга для корпоративной сети ТюмГНГУ.

Литература

1. *Информационные* технологии в образовательном процессе: Материалы обл. межвуз. науч.-метод. конф. 5 апр. 2002 г. Тюмень: Вектор-Бук, 2002. С. 88–97.

2. *NetFlow //* http://www.cisco.com/warp/public/cc/cisco/mk t/ios/netflow/tech/napps_wp.htm.

3. *Aboba B., Arkko J., Harrington D.* Introduction to Accounting Management. RFC 2975.

4. *Travostino F.* Towards Active IP Accounting Infractructure. OpenArch. Tel Aviv, 2000.

R. N. Zalata

AGGREGATION AND STATISTICAL PRE-PROCESSING OF ACCOUNTING INFORMATION WITH A VIEW OF OPTIMIZING OPERATIONS WITH DATABASE MANAGEMENT SYSTEM (DMS) DESIGNED FOR ACCOUNTING SYSTEMS AND MONITORING CORPORATE NETWORKS

In the course of creating monitoring systems and calculating traffic for corporate networks, one faces a problem of a big volume of stored and processed data (accounting information) resulting in excessive consumption of computing resources by such systems. The article quotes algorithms of statistical pre-processing of accounting information leading to considerable economy of DMS resources and several times increasing operational capacity. The algorithms are validated by experimental data also quoted in the paper.