ПРЕДВАРИТЕЛЬНЫЕ РЕЗУЛЬТАТЫ ТЕСТИРОВАНИЯ СОЗДАВАЕМОЙ СИСТЕМЫ МОНИТОРИНГА И СБОРА СТАТИСТИКИ СПД СО РАН*

Ю. И. Шокин, С. Д. Белов, Л. Б. Чубаров
Институт вычислительных технологий СО РАН, Новосибирск, Россия
e-mail: shokin@ict.nsc.ru, belov@nsc.ru, chubarov@ict.nsc.ru

Main results of testing for the efficiency, reliability and productivity characteristics of the server intended for the statistics data gathering for the Data Exchange System of SB RAS are presented in this paper. This server is intended to early detect any malicious influences and attacks from the outside networks. It also deals with a detection of an anomalous behavior of internal computers and with an identification of non-legitimate applications in order to provide a sufficient level of the network security in general. For the preliminary evaluation of the capabilities of the software/hardware complex being built, the procedure of calibration of the system was carried out. It is proved that the selected hardware platform and operating system along with the set of different collector programs support sufficient throughput. This complex is capable to process the analyzed data flow by avoiding the loss of packets and providing the trustworthiness of gathered data upon the current channel loads. At the same time the average processor load doesn't exceed a few percents. These tests run of the system have demonstrated sufficient completeness of the gathered statistical information and its adequacy to the stated goals.

Введение

В статье излагаются результаты исследования работоспособности, надежности и производительности сервера сбора статистики сети передачи данных СО РАН, установленного в центральном узле СПД в начале марта 2007 г. Этот сервер предназначен для раннего обнаружения вредоносных воздействий на сеть извне, проявлений аномального поведения компьютеров абонентов сети и наличия нелегитимных приложений с целью обеспечения приемлемого уровня безопасности сети в целом. Важность оценки эффективности установленной на сервере операционной системы и прикладных программ в

*Работа выполнена при поддержке Российского фонда фундаментальных исследований (грант № 06-07-89038), Программы интеграционных фундаментальных исследований СО РАН (проект № 1.7), Программы государственной поддержки научных исследований, проводимых ведущими научными школами Российской Федерации (проект № НШ-9886.2006.9), государственного контракта № 2007-4-1.4-00-04-103.

части обработки сетевых потоков без просчетов и пропусков обусловлена намерением использовать сервер для анализа потоков данных значительной интенсивности в режиме реального времени.

1. Внешние подключения системы передачи данных СО РАН

В настоящее время интенсивность подвергаемых анализу потоков достигает 150 Мбит/с, или около 30–40 тыс. пакетов в 1 с. Графики загрузки внешних каналов СПД СО РАН (рис. 1 и 2) иллюстрируют эту загрузку в интервале с 03:30 24.07.2007 по 13:00 25.07.2007 для типичных рабочих дней. На графиках тонкой черной линией (в оригинале она синяя) обозначен исходящий трафик каждого из каналов, сплошной серой заливкой (в оригинале зеленой) — входящий. Максимальная пропускная способность каждого подключения в настоящей конфигурации составляет 100 Мбит/с, в подписях к графи-

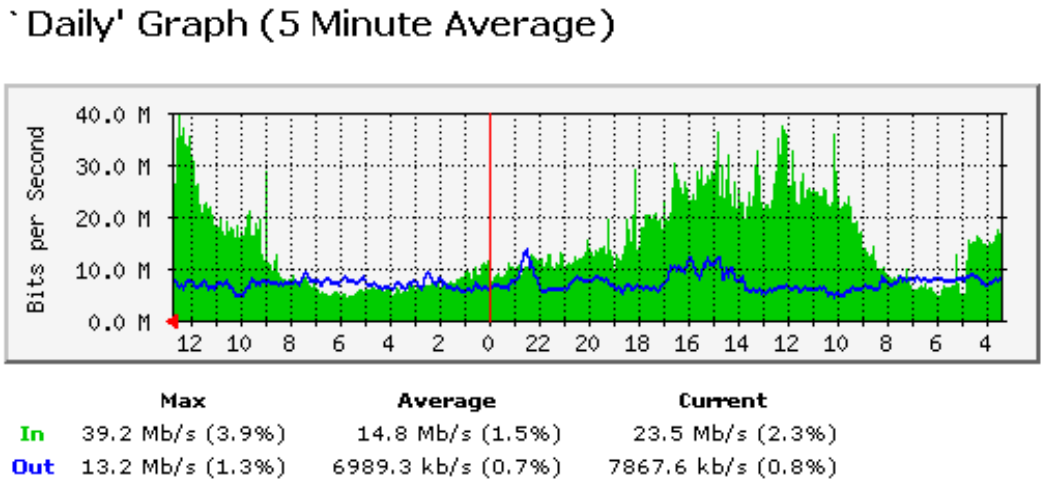

Рис. 1. График загрузки первого канала внешнего подключения

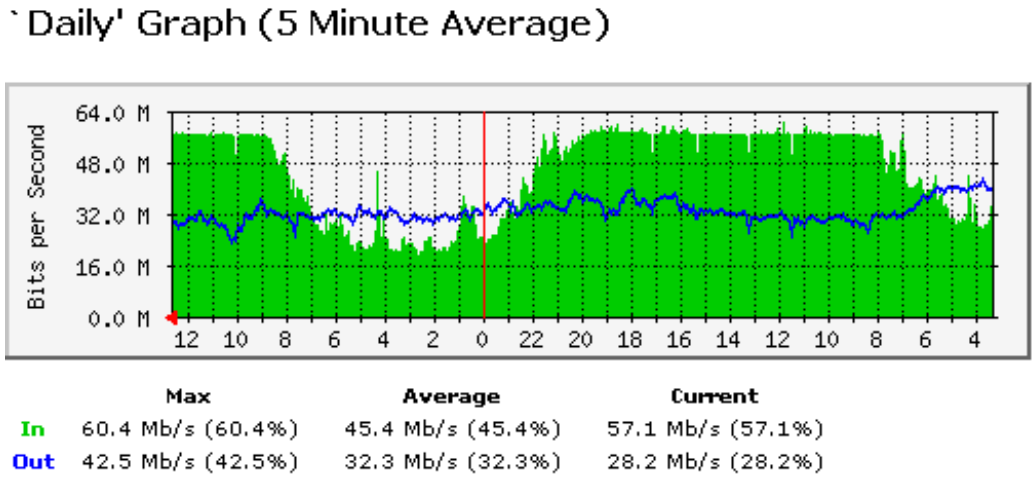

Рис. 2. График загрузки второго канала внешнего подключения

Таблица 1. Фрагмент файла, содержащего исходные “сырые” статистические данные

195.138.76.51	193.124.167.14	1	368
85.198.129.82	193.124.167.14	1	168
87.10.1.245:443	193.124.167.14:19345	6	205
193.233.79.247:80	193.124.167.14:29471	6	45052
193.233.79.247:80	193.124.167.14:18122	6	16191
193.233.79.247:80	193.124.167.14:45527	6	16933
84.252.139.249:80	193.124.167.14:44823	6	1420
89.108.91.250:80	193.124.167.14:40334	6	13429
89.108.91.251:80	193.124.167.14:35593	6	19493

кам максимальное, среднее и текущее значения трафика в каждом из направлений, в мегабитах в секунду и в процентах от максимальной емкости канала. Различная загруженность каналов определяется схемами административного взаимодействия СО РАН с сетевыми провайдерами Информика и РБНет. На графиках отчетливо видно понижение сетевой активности в ночные часы, ее значительное возрастание в начале рабочего дня до фактического насыщения одного из каналов на протяжении всего рабочего дня с 08:00 до позднего вечера, после чего сетевая активность значительно снижается. Полный трафик, пропущенный через внешние подключения СПД, в рабочие дни составляет 1.25 Тб данных.

Файл, содержащий исходные “сырые” статистические данные, соответствующие интервалу с 12:55 до 13:00 25 июля 2007 г., имеет полный объем более 25 Мбайт и содержит более 500 тыс. записей следующего вида (табл. 1). Здесь в первой колонке приводится в зависимости от IP-протокола (колонка 3) IP-адрес источника, во второй — IP-адрес приемника, в третьей — номер IP-протокола (1 — ICMP, 6 — TCP, 17 — UDP и т.д.), в четвертой — счетчик байтов данного потока (flow). Для протоколов, в которых определено понятие портов (TCP, UDP), IP-адреса сопровождаются значениями соответствующих портов, отделенных от адреса символом двоеточия.

2. Сервер мониторинга и обработки статистических данных

Сервер построен на основе современного двухпроцессорного компьютера (Xeon 3.20 GHz), оснащенного 4 Гб оперативной памяти, тремя сетевыми Ethernet-интерфейсами: 100 Мбит/с в качестве системного интерфейса и двумя гигабитными — в качестве мониторирующих. Исследуемый поток передается с центрального коммутатора сети СО РАН с использованием технологии span-портов (мониторирующих портов), когда на один из интерфейсов коммутатора/маршрутизатора копируется весь трафик некоторых выделенных интерфейсов.

Примененная схема обладает рядом недостатков, таких как плохая масштабируемость, повышенная нагрузка на активное оборудование инфраструктуры сети, искажение временных характеристик исследуемого трафика. Проблемы мониторинга каналов значительной емкости при больших загрузках подробно проанализированы в работах [1, 2]. Поэтому после получения доступа к специализированному диагностическому оборудованию планируется провести перестройку данной схемы.

В сетевом сообществе отмечается определенный интерес к вопросам эффективного мониторирования современных высокопроизводительных сетей, в частности, с использованием технологии полного захвата исследуемого потока (сниффинг) при высоких загрузках, с использованием распространенного неспециализированного оборудования [3, 4]. Эффективность такой технологии определяется используемыми аппаратными средствами и программным обеспечением. Для масштабируемости системы мониторинга, т. е. для возможности ее стабильной работы с ростом уровня загрузки сети, требуется тщательная оценка характеристик создаваемой системы.

Неадекватность системы захвата трафика может проявляться по-разному: во-первых, в системе могут возникать потери пакетов, когда не все приходящие на мониторирующий интерфейс пакеты оказываются прочитанными; во-вторых, может проявиться нехватка вычислительных ресурсов для последующего анализа захваченных пакетов — нехватка оперативной памяти или процессорного времени. Вероятность потери пакетов может быть уменьшена за счет правильного выбора сетевого интерфейса. Как правило, распространенные сетевые адаптеры, широко применяемые в настольных системах, требуют дополнительных затрат процессорного времени при чтении принятых пакетов и потому значительно уступают в производительности специализированным серверным вариантам. Использование в построенной системе серверных сетевых интерфейсов на базе Intel PRO/1000 PT (80003ES2) уменьшает вероятность потери пакетов и обеспечивает более эффективную работу по оптимизации обработки прерываний, по управлению внутренними буферами интерфейса и т. п.

Проведенное исследование, названное нами калибровкой системы, показало, что установленная ОС в комплексе с различными программами-коллекторами обладает достаточной производительностью, обрабатывая анализируемый поток без потерь пакетов, и тем самым достигается достоверность собираемых данных при существующей загрузке каналов. Отсутствие просчетов (потерь пакетов) подтверждается результатами проведенных измерений, когда в сеть запускался “калибровочный” поток информационных пакетов, генерируемых на одной из внутренних машин сети и адресованных некоторой внешней машине, не входившей в состав сети, так что этот трафик должен был фиксироваться системой мониторинга. Было организовано несколько сессий передачи тестового трафика между “внутренней” машиной xbeta.nsc.ru и машиной npd.ac.ru, расположенной в здании Президиума РАН (Москва).

В каждой из сессий, которые проводились в рабочее время, т. е. в периоды максимальной загрузки сети, передавался 1 млн пакетов, генерированных программным пакетом HPING. Факт фиксации калибровочного потока системой мониторинга подтверждался параметрами собранной статистики для указанных хостов и специально запускавшимися сессиями программы TCPDUMP, явно фиксировавшими калибровочный трафик. В результате измерений не было зафиксировано даже единичных просчетов.

3. Сбор и обработка данных сетевой статистики

Программы-коллекторы анализируют атрибуты каждого пакета, передаваемого по внешним каналам СПД, и содержащиеся в пакете данные. Таких программ может быть несколько, и работать они могут параллельно. Суть проводимого анализа состоит в том, что программа-коллектор, занимающаяся сбором статистики трафика, суммирует

объем пакетов с одинаковыми атрибутами и сохраняет аккумулированную на заданном временном интервале статистику в дисковых файлах. Рассматривалось несколько вариантов программ-коллекторов (CFLOWD, TRAFD, CNUPM), которые можно было бы применить в дальнейшей работе для сбора статистики по использованию канальной емкости. По результатам испытаний была выбрана программа CNUPM, обеспечивающая минимальную загрузку процессора и, стало быть, максимальную производительность, что позволяет дополнительно задействовать другие специализированные коллекторы. Так, программа CNUPM оставляет доступными для других коллекторов около 95 % ресурса процессора, в то время как система SNORT с ограниченной библиотекой сигнатур оставляет только 90 %, а с полной библиотекой — занимает процессор полностью.

Статистические данные, на основе которых в дальнейшем генерируются отчеты об использовании абонентами канальной емкости, включают следующие атрибуты IP-трафика: адреса отправителя и получателя, тип IP-протокола (TCP, UDP, ICMP и т. п.), номера портов для протоколов, в которых это понятие определено, и суммарный объем пакетов. Объем собираемых статистических данных достаточно велик, его характерная величина для СПД СО РАН составляет около 1 Гб в сутки компрессированных данных. Это обстоятельство при генерации отчетов за определенный период времени требует дополнительной обработки с помощью достаточно простых средств, например, интерпретируемых скриптов на языках AWK, Perl. Разработано несколько таких скриптов для генерации в текстовом и в HTML-форматах периодических отчетов об использовании ресурсов “внутренними” машинами и “внешними” абонентами сети. В ходе обработки происходят агрегирование записей, их группирование по абонентам-организациям, сортировка по внутренним машинам абонента и по суммарному его трафику. Применение механизма ассоциативных массивов, включенного в упомянутые выше языки программирования, позволило сократить продолжительность обработки в несколько раз, до 1.5 ч.

Другие коллекторы могут анализировать не только сетевые атрибуты пакета, но и содержащиеся в пакетах данные (payloads). Так, для идентификации протокола передачи электронной почты достаточно обнаружить в анализируемой последовательности пакетов несколько ключевых слов, характерных для этого протокола (HELO, EHLO, MAIL FROM, RCPT TO). В качестве программ-коллекторов, анализирующих передаваемые данные, применялись программа URLSNARF, являющаяся компонентом пакета DSNIFF [5], и система SNORT [6]. Отметим, что CNUPM собирает интегральную статистику трафика, программа URLSNARF выделяет из анализируемого потока характерные запросы http GET, используемые программами, которые работают в протоколе BitTorrent, а программа SNORT отлавливает сигнатуры, характерные для протокола EDonkey.

Поскольку система SNORT в основном ориентирована на распознавание вторжений, вирусных атак и прочих угроз, а не на анализ трафика и идентификацию прикладных протоколов, ее библиотека сигнатур должна быть существенно пересмотрена и сокращена. На начальном этапе работы рассматривался ограниченный набор сигнатур, необходимых для идентификации только двух сетевых приложений E-Donkey и BitTorrent, относящихся к категории наиболее важных в наших условиях Peer-To-Peer-приложений, ответственных, по предварительным оценкам, за генерацию до 20–30 % нелегитимного трафика. Анализируя характерную структуру HTTP-запроса GET, использующегося в протоколе BitTorrent, можно получить количественные данные об объемах трафика, связанного с этим приложением.

Таблица 2. Распределение долей трафика по протоколам

Протокол	Доля в трафике, %
6 (TCP)	93.7
17 (UDP)	6.1
1 (ICMP)	0.16

Принимая во внимание доминирующую роль протокола передачи данных TCP в современном Интернете, необходимо серьезно отнестись к особенностям анализа этого протокола в системах мониторинга. В табл. 2 приведены данные, характеризующие ситуацию обычного рабочего дня 25 июля 2005 г., 12-55 (Нск), по СПД СО РАН.

Ранее было отмечено [7], что в большинстве систем анализа трафика, будь то IDS или другие специализированные системы, недостаточное внимание уделяется проблемам однозначной реконструкции прикладного потока данных TCP на основании последовательности IP-пакетов анализируемого трафика. Основные проблемы этой реконструкции связаны с неоднозначностями спецификаций протокола TCP, а также с особенностями реализации протокола TCP в различных операционных системах [8]. Например, при наличии фрагментированных IP-пакетов разные операционные системы по-разному трактуют присутствие "повторенных" данных. При этом могут использоваться либо принятые ранее данные, либо данные, принятые позже, что приводит к некорректной работе системы анализа трафика.

Опытная эксплуатация системы показала, что собираемые ею данные достоверны и не противоречат данным локальных систем сбора статистики, установленных в сетях некоторых абонентов.

Примеры типичного суточного отчета по СПД СО РАН, формируемого разрабатываемой системой, приводятся в табл. 3–5. В этом отчете содержатся данные о загрузке

Таблица 3. СПД СО РАН в целом

NSC traffic report — 2007.07.24

Top 15 traffic-consuming hosts:

1	44,707,219,815	3.56 %	3.56 %	11.34 %<	194.226.183.151	ihttm
2	43,245,336,149	3.44 %	7.00 %	94.98 %<	84.237.116.5	ik
3	40,536,762,559	3.23 %	10.23 %	31.86 %<	194.226.177.248	isi
4	28,555,135,097	2.27 %	12.50 %	70.38 %<	217.79.57.161	tomsk
5	27,706,668,684	2.21 %	14.71 %	9.02 %<	212.192.164.11	nsu
6	26,898,414,791	2.14 %	16.85 %	26.78 %<	193.124.39.47	inh
7	26,040,172,525	2.07 %	18.92 %	86.18 %<	84.237.20.138	irkut
8	26,026,161,021	2.07 %	20.99 %	78.79 %<	212.192.163.20	tomsk
9	24,276,445,931	1.93 %	22.92 %	8.17 %<	194.85.127.68	ihkg
10	22,961,160,628	1.83 %	24.75 %	94.89 %<	217.79.61.36	bb
11	18,841,712,212	1.50 %	26.25 %	49.97 %<	217.79.61.7	bb
12	17,975,517,187	1.43 %	27.68 %	93.65 %<	84.237.18.129	irkut
13	17,706,225,151	1.41 %	29.09 %	91.11 %<	193.124.167.14	binp
14	16,214,203,544	1.29 %	30.38 %	81.54 %<	84.237.20.66	irkut
15	15,603,299,617	1.24 %	31.62 %	94.37 %<	212.192.189.126	oiggm

Started: 00:30 Finished: 1:37

Total traffic: 1,256,309,511,165 Hosts: 59,569 Flows: 156,696,838

сети в целом, список наиболее активных хостов сети с указанием их принадлежности к организации либо региональному филиалу (абоненту). Даже предварительный анализ данных, содержащихся в этих таблицах, показывает, что около трети трафика генерируется всего 15 хостами (из почти 60 тыс. работавших в сети). Полный объем такого "краткого" отчета составляет около 50 страниц.

В первом столбце табл. 3 указаны номера записей, во втором — суммарный трафик хоста, принадлежащего организации-абоненту, в третьем — доля этого хоста в общем трафике СПД СО РАН, в четвертом — "накопленный процент", т. е. суммарная доля текущего и предшествующих ему в отчете хостов, в пятом — доля принимаемого хостом трафика от его же общего трафика (направленность трафика, in/out), в шестом — IP-адрес хоста, в седьмом — условное имя абонента, в сеть которого входит хост.

Полное время анализа суточных статистических данных составляет около 1.5 ч. Следует отметить, что, поскольку анализируется "живой" трафик сети, доля трафика неактивных хостов (т. е., например, попытки сканирования извне неактивных в настоящее время адресов) приводит к определенному завышению количества учтенных хостов. Для устранения этой систематической погрешности необходимо несколько усложнить алгоритмы обработки.

В табл. 4 и 5 приведены количественные характеристика трафика внутри организации-абонента. Содержание этих таблиц, с учетом отсутствия "первого" и "седьмого" столбцов, аналогично содержанию предыдущей с той лишь разницей, что все доли вычисляются по отношению к суммарному трафику абонента. Для каждого абонен-

Таблица 4. Иркутский научный центр

Traffic of Irkutsk (irkut):
Traffic: 206,398,949,738 Hosts: 4,120 Flows: 21,712,999
Inbound: 147,381,940,519 In/Out: 71.41 %< Of total: 13.86 %
Outbound: 59,017,009,219 Of total: 16.43 % Cum: 16.43 %

26,040,172,525	12.62 %	12.62 %	86.18 %<	84.237.20.138
17,975,517,187	8.71 %	21.33 %	93.65 %<	84.237.18.129
16,214,203,544	7.86 %	29.18 %	81.54 %<	84.237.20.66
15,548,075,993	7.53 %	36.71 %	3.84 %<	84.237.20.2
14,110,711,576	6.84 %	43.55 %	60.52 %<	84.237.20.10
14,001,015,883	6.78 %	50.33 %	86.84 %<	84.237.20.146
13,255,191,494	6.42 %	56.76 %	97.10 %<	84.237.25.65
9,989,461,015	4.84 %	61.60 %	91.84 %<	84.237.20.134
9,203,417,542	4.46 %	66.06 %	38.75 %<	84.237.19.7
7,575,479,820	3.67 %	69.73 %	94.92 %<	84.237.25.145
6,594,820,334	3.20 %	72.92 %	84.70 %<	84.237.22.249
5,056,015,026	2.45 %	75.37 %	94.77 %<	84.237.17.73
3,865,642,535	1.87 %	77.24 %	60.04 %<	84.237.21.149
3,576,506,797	1.73 %	78.98 %	3.00 %<	84.237.21.144
3,407,135,811	1.65 %	80.63 %	90.11 %<	84.237.25.8
3,406,500,149	1.65 %	82.28 %	75.50 %<	84.237.23.37
2,364,354,463	1.15 %	83.42 %	88.41 %<	84.237.19.5
2,216,830,366	1.07 %	84.50 %	4.16 %<	84.237.19.10
2,090,493,198	1.01 %	85.51 %	77.30 %<	84.237.24.10
1,810,618,187	0.88 %	86.39 %	85.42 %<	84.237.30.6

Таблица 5. Томский научный центр

Traffic of Tomsk (tomsk):
Traffic: 167,391,548,598 Hosts: 4,360 Flows: 25,228,888
Inbound: 113,043,204,246 In/Out: 67.53 %< Of total: 16.10 %
Outbound: 54,348,344,352 Of total: 13.32 % Cum: 29.75 %

28,555,135,097	17.06 %	17.06 %	70.38 %<	217.79.57.161
26,026,161,021	15.55 %	32.61 %	78.79 %<	212.192.163.20
12,571,823,892	7.51 %	40.12 %	92.44 %<	217.79.57.183
12,432,922,085	7.43 %	47.54 %	23.83 %<	84.237.0.206
11,145,188,148	6.66 %	54.20 %	84.94 %<	84.237.1.35
8,937,537,691	5.34 %	59.54 %	76.98 %<	212.192.163.22
8,663,904,026	5.18 %	64.72 %	25.00 %<	212.192.163.179
7,456,421,113	4.45 %	69.17 %	70.39 %<	84.237.0.26
5,914,925,516	3.53 %	72.71 %	38.96 %<	84.237.1.90
4,694,800,857	2.80 %	75.51 %	92.09 %<	84.237.1.97
3,687,032,028	2.20 %	77.71 %	71.33 %<	217.79.57.132
3,114,343,987	1.86 %	79.57 %	93.56 %<	84.237.1.161
2,970,063,749	1.77 %	81.35 %	51.30 %<	212.192.163.10
2,911,431,106	1.74 %	83.09 %	38.29 %<	84.237.4.12
2,586,527,532	1.55 %	84.63 %	93.42 %<	84.237.0.10
2,332,077,580	1.39 %	86.03 %	8.33 %<	217.79.57.141
2,064,490,704	1.23 %	87.26 %	93.22 %<	217.79.57.184
1,999,242,191	1.19 %	88.45 %	93.10 %<	217.79.57.131
1,963,186,223	1.17 %	89.63 %	88.23 %<	84.237.0.254
1,645,240,774	0.98 %	90.61 %	93.88 %<	217.79.57.189

та в данном отчете приводятся лишь первые 20 хостов (также доступен и полный отчет по трафику абонентов). Позиции заголовка таблиц:

Traffic — полный учтенный трафик данного абонента;

Hosts — количество зафиксированных в трафике хостов, принадлежащих к сетям данного абонента (с учетом вышеприведенного замечания о неактивных хостах);

Flows — количество записей системы сбора статистики, относящихся к хостам данного абонента (с учетом предыдущей оговорки);

Inbound и **Outbound** — соответственно входящий и исходящий трафики абонента;

Cum — доля, которую обеспечили в общем потреблении трафика данный абонент и все предыдущие в этом отчете.

Заключение

Наблюдение за характером использования сети абонентами и отдельными хостами позволяет обнаруживать атипичный трафик и проводить необходимое расследование. Следует заметить, однако, что существуют программные средства, способные организовать фрагментацию сетевого трафика пользовательского компьютера, и эти методы “обмана” широко распространены. Подобные ситуации должны быть по крайней мере идентифицированы системой анализа, что требует модификации ее системного кода. Такая работа запланирована на будущее.

Список литературы

[1] Сеть передачи данных СО РАН // Информационные материалы научно-координационного совета целевой программы "Информационно-телекоммуникационные ресурсы СО РАН". Новосибирск, 2005.

[2] Шокин Ю.И., Федотов А.М., Белов С.Д., Зайцев А.С., Никульцев В.С., Чубаров Л.Б. Проблемы мониторинга и сбора статистики в больших корпоративных научно-образовательных сетях на примере СПД СО РАН // Вест. ИрГТУ. 2006. Т. 3, № 2(26). С. 6–16.

[3] Schneider F., Wallerich J. Performance Evaluation of Packet Capturing Systems for High-Speed Networks // CoNEXT '05: Proceedings of the 2005 ACM conference on Emerging Network Experiment and Technology. France: Toulouse, 2005. P. 284–285.

[4] Varenni G., Baldi M., Degioanni L., Risso F. Optimizing packet capture on symmetric multiprocessing machines // Proc. of 15th Symp. on Computer Architecture and High Performance Computing, 2003. 10–12 Nov. 2003. P. 108–115.

[5] http://monkey.org/~dugsong/dsniff/

[6] http://www/snort.org/

[7] Ptacek T.H., Newsham T.N. Insertion, Evasion, And Denial Of Service: Eluding Network Intrusion Detection // Technical Report, Secure Networks, Inc., Jan. 1998.

[8] Handley M., Kreibich C., Paxson V. Network Intrusion Detection: Evasion, Traffic Normalization, and End-to-End Protocol Semantics // Proc. USENIX Security Symp. 2001.

Поступила в редакцию 30 июля 2007 г.,
в переработанном виде — 6 сентября 2007 г.