УДК 004.735
В.В. Милюков, доцент, канд. техн. наук
С.А. Зуев, доцент, канд. техн. наук
С.В. Покрова
Таврический национальный университет имени В.И. Вернадского
пр. Вернадского 4, г. Симферополь, Республика Крым, Россия, 295004
sazuev@ya.ru, pokrova_sophiya@mail.ru

СИСТЕМНО-ФУНКЦИОНАЛЬНЫЙ АНАЛИЗ ПОТОКОВ ДАННЫХ В СЕТЯХ ИНТЕРНЕТ-ПРОВАЙДЕРОВ КРЫМА[17]

В работе рассмотрены базовые методы системного и функционального анализа сетевого трафика, позволяющие получить статистические данные для разработки методик оптимизации и управления качеством обслуживания в мультисервисных сетях. Выполнен системный анализ маршрутов передачи данных провайдеров Крыма и получены их функциональные характеристики.
***Ключевые слова**: потоки данных, сетевые анализаторы, анализ трафика.*

Введение. На сегодняшний день в связи с особенностью статуса нашего региона, возникают задачи организации и оптимизации интернет-каналов связи. Провайдеры Республики Крым пока не перестроились на каналы Российских Интернет-провайдеров. Кроме того несколько поменялась направленность запросов пользователей на территории Крыма. К примеру, изменились популярные интернет магазины, поменялись информационные порталы и т.п. Все это в совокупности привело к избыточным задержкам в сетях провайдеров в результате увеличения количества транзитных маршрутизаторов и перегрузке каналов, не оптимизированных под новые потоки данных. Таким образом, становится актуальной задача анализа трафика местных провайдеров и поиск решения по оптимизации маршрутов.

Данная научно-техническая проблема может эффективно решаться посредством имитационного моделирования потоков трафика. Однако такое решение предполагает статистический анализ и мониторинг существующих каналов связи, анализ потоков информации, результатом которого и могут стать какие-либо рекомендации по организации новых каналов связи.

Целью данной работы является анализ методов мониторинга сетевых каналов и сетевого трафика как в локальных сетях, так и сетях интернет провайдеров и сбор статистики о используемых каналах активными провайдерами Республики Крым.

Подробный анализ сетевого трафика позволит решить задачи оптимизации, модернизации сетевой инфраструктуры, обеспечения заданного приемлемого качества обслуживания и безопасности в сетях провайдеров Крыма.

Типичные задачи анализа сетевого трафика [2]:

- анализ загрузки системы, например, как часто определенные порты используются такими протоколами, как FTP или HTTP при подключении к серверу, как используется полоса пропускания различными приложениями, как отдельные пользователи или группы пользователей используют полосу пропускания;
- анализ характеристик сетевого трафика, таких как среднее время жизни и размер пакетов, отношение между числом потерянных пакетов и временем жизни пакетов и т.д.;
- анализ характеристик сессий, таких как длительность взаимодействия клиентов с веб-серверами, время отклика веб-серверов на клиентские запросы, продолжительность использования пользователями интернет-сервисов и т.д.

Вышеперечисленные задачи предъявляют важные функциональные требования к средствам мониторинга и анализа, такие как способность взаимодействия протоколов всех уровней эталонной модели ISO OSI, включая прикладной уровень. При этом одним из важных требований, которые предъявляются к этим средствам, является возможность анализа сетевого трафика в реальном масштабе времени.

Как указывалось в [2], мониторинг трафика жизненно важен для эффективного управления сетью. Он является источником информации о функционировании корпоративных приложений, которая учитывается при распределении средств, планировании вычислительных мощностей, определении и локализации отказов, решении вопросов безопасности.

Одной из актуальных научных задач в настоящее время является анализ (и дальнейшее прогнозирование) самоподобной структуры трафика в современных мультисервисных сетях. Для решения этой задачи необходим сбор и последующий анализ разнообразной статистики (скорость,

[17] Работа выполнена при финансовой поддержке РФФИ (грант № 14-41-01564).

объемы переданных данных и т.д.) в действующих сетях. Сбор такой статистики в том или ином виде возможен различными программными и программно-аппаратными средствами. Среди них можно выделить следующие группы

- Исследование трафика с помощью анализаторов
- Исследование с помощью протокола SNMP агентов
- Исследование статистики, накопленной методом трассировок, с целью изучения временных зависимостей.

Рассмотрим основные методики, определим область использование каждой.

Анализ потоков данных с использованием сетевых анализаторов. Основой работы сетевых анализаторов является принцип их действия, который заключается в перехвате трафика и обработке полученной информации. Сетевые анализаторы принято называтьснифферами.

Снифферы – это программные или аппаратно-программные комплексы, решающие задачи

- предоставления информации о количестве пользователей, зарегистрированных в сети и количестве генерируемого трафика;
- идентификации используемого программного обеспечения и обнаружения несанкционированного программного обеспечения;
- прослушивания трафика и локализации несанкционированного трафика;
- анализа нагрузки, вызванной подключением нового пользователя;
- локализации трудноразрешимых проблем;
- обнаружения и идентификации несанкционированного программного обеспечения;
- идентификации неиспользуемых протоколов для удаления их из сети;
- получения такой информации, как базовые модели трафика и метрики утилизации сети;
- генерации трафика для испытания на вторжение с целью проверки системы защиты;
- работы с системами обнаружения вторжений IntrusionDetectionSystem (IDS);
- изучения работы сети.

Все перечисленные задачи особенно актуальны в связи распространениеммультисервисных сетей, так как они предъявляют более жесткие требования к потокам передачи данных. Необходимо своевременно детектировать неполадки и правильно настраивать приоритетность трафика, так как голосовой трафик очень чувствителен к временным задержкам и джиттеру. Использование сетевых анализаторов открывает уникальные возможности по оптимизации по обеспечению надежности и информационной безопасности, поддержки работоспособности сетей.

Работу сетевого анализатора можно разбить на несколько последовательных этапов.

Первым этапом работы сниффера является перехват данных. Можно использовать различные механизмы перехвата от внедрения в линию связи до атаки канального и сетевого уровня, приводящие к перенаправлению трафика на узел со сниффером.

Далее происходит декодирование и сохранение полученной информации.Можно извлекать данные не только из заголовков пакетов, но и изучать содержимого пакетов.

Основным этапом работы является анализ. Увеличение объема трафика требует более тщательного анализа не только в режиме реального времени (анализ отдельных пакеты), но и восстановление сессии (установление взаимосвязей между тысячами отдельных пакетов и объединение их по принадлежности к отдельным приложениям). Объемы трафика в таком случае требует использования экспертных систем для автоматизации анализа. Анализ может производиться в режиме реального времени или по сохраненному трафику.

На рынке представлены различные продукты, поэтому необходимо понимать какие задачи должен решать конкретный анализатор в сети.

В [2] подробно описаны характеристики ряда широко распространенных сетевых анализаторов. На наш взгляд этот список может быть несколько расширен и дополнен.

1) Утилита tcpdump является самом простым и удобным средством отладки проблем в сети, позволяющим перехватывать и анализировать сетевой трафик, проходящий через компьютер, на котором запущена данная программа.Она, как правило, используется как сниффер прежде всего пакетов, а не сетевых потоков, так как не восстанавливает сессии в автоматическом режиме.

2) Функциональность, которую предоставляет Wireshark, схожа с возможностями программы tcpdump, однако Wireshark имеет графический пользовательский интерфейс и гораздо больше возможностей по сортировке и фильтрации информации. Wiresharkявляется кроссплатформенным продуктом с открытым кодом и распространяется абсолютно бесплатно. Позволяет перехватывать и декодировать трафик с использованием гибких правил фильтрации, применяемых на любых типах интерфейсов. Преимуществом Wireshark является способность импортировать данные из файлов сессий, созданных другими анализаторами, и возможность сохранять свои данные в различных форматах,

доступных для импорта другими программами. Показывает хорошие результаты при восстановлении сессии в связи с тем, что поддерживает большое количество сетевых протоколов.

3) IrisNetworkTrafficAnalyzer помимо стандартных функций сбора, фильтрации и поиска пакетов, а также построения отчетов, программа предлагает уникальные возможности для реконструирования данных. В модуле дешифрования (decodemodule) преобразует сотни собранных двоичных сетевых пакетов в единое пользовательское сообщение. IrisTheNetworkTrafficAnalyzer помогает детально воспроизвести сеансы работы пользователей с различными web-ресурсами и даже позволяет имитировать отправку паролей для доступа к защищенным web-серверам с помощью cookies, расширяя возможности имеющихся средств мониторинга и аудита. Анализатор пакетов Iris позволяет зафиксировать различные детали атаки, такие как дата и время, IP-адреса и DNS-имена компьютеров хакера и жертвы, а также использованные порты.

4) Snort — это кроссплатформенная система обнаружения вторжений, распространяемая с открытым исходным кодом. ПО Snort выполняет протоколирование, анализ, поиск по содержимому. Широко используется для активного блокирования или пассивного обнаружения целого ряда атак и зондирований, таких как попытки атак на переполнение буфера, скрытое сканирование портов, атаки на веб-приложения, SMB-зондирование и попытки определения операционной системы. Программное обеспечение в основном используется для предотвращения проникновения и блокирования атак, если они имеют место.

В источниках [2,4] рассмотрены архитектурные особенности, преимущества и недостатки систем анализа сетевого трафика, а также проведен сравнительный анализ некоторых из них.

Использование протокола SNMP для мониторинга сети. В недалеком прошлом мониторинг трафика был относительно простой задачей. Как правило, компьютеры объединялись в сеть на основе шинной топологии, т. е. имели разделяемую среду передачи. Это позволяло подсоединить к сети единственное устройство, с помощью которого можно было следить за всем трафиком. Однако требования к повышению пропускной способности сети и развитие технологий коммутации пакетов, вызвавшее падение цен на коммутаторы и маршрутизаторы, обусловили быстрый переход от разделяемой среды передачи к высокосегментированным топологиям. Общий трафик уже нельзя увидеть из одной точки. Для получения полной картины требуется выполнять мониторинг каждого порта. Использование соединений типа «точка-точка» делает неудобным подключение таких устройств к портам, да и понадобилось бы слишком большое их число для прослушивания всех портов, что превращается в чересчур дорогостоящую задачу. Вдобавок сами коммутаторы и маршрутизаторы имеют сложную архитектуру, и скорость обработки и передачи пакетов становится важным фактором, определяющим производительность сети.

В святи с этим была разработана методика, использующаяпрограммных агентов, которые установлены на каждом узле и предоставляют данные по запросу с минимальными нагрузками на рабочую станцию. Такой метод мониторинга сети в режиме реального времени основан на использовании и опросеSNMP-агентов, установленных на коммуникационном оборудовании. Полученные данные отображаются в виде графиков, что наглядно позволяет отслеживать состояние сети, видеть пиковые ситуации и реагировать

Существует несколько свободно распространяемых решений MRTG,Cacti, Zabbix, Nagios, а также коммерческие предложения Ganglia, Tivoli.

В [2] представлено сравнение пяти открытых программных систем анализа трафика методом опроса SNMP-агентов. Сравнительный анализ решений позволяет отдать предпочтение MRTG за простоту настройки и использования, Zabbix за его функциональность.

Метод прямой трассировки сети. Утилита tracert или traceroute является достаточно простым инструментом, входящим в состав любой операционной системы. Метод трассировки узлов сети позволяет определить маршрут передачи пакета и сделать выводы о возможных проблемах и временных характеристиках сети. Однако при анализе результатов следует помнить, что задержка, которую отображает данная утилита, является комплексной величиной, учитывающая не только задержку на распространение, но и ряд других факторов. Трассировка позволяет получить суммарные задержки в обе стороны передачи данных (от клиента к серверу и от сервера к клиенту), хотя, как правило, доставка пакетов производится разными маршрутами. Наличие балансировки нагрузки в магистральных каналах связи тоже приводят к неоднозначности интерпретации результатов. Однако, несмотря на все сложности и неоднозначности, описанные в [3], использование этой утилиты позволяет получить общую картину задержек при достаточном количестве испытаний и усредненных значениях.

Круг решаемых задач определил целесообразность использования этого метода на первом этапе исследования. Для решения поставленной задачи необходимо было начать с трассировки. Для определения направления передачи данных и формирования данных о маршрутах передачи основного объема трафика был сформирован список наиболее посещаемых сайтов Крыма и проанализированы маршруты различных Интернет-провайдеров. Результаты экспериментальных исследований представлены в таблицах 1 и 2.

Таблица 1 – Временные задержки при трассировке удаленных серверов

	www.yandex.ru	www.google.com	meta.ua	vk.com	odnoklassniki.ru	www.youtube.com	mail.ru	wikipedia.org	facebook.com	www.avito.ru	www.gismeteo.ru	slando.ua
FreeNet	41	89	23	48	43	23	42	64	153	71	55	79
FreeNet 2 канал	151	77	26	66	55	35	60	73	178	115	346	83
Воля	719	470	719	605	569	326	961	548	516	455	601	366
Ардинвест	36	43	15	41	31	13	32	47	143	87	31	75
Ардинвест 2 канал	36	52	16	51	34	-	32	48	48	93	33	74
Ардинвест 3 канал	35	45	16	41	34	14	34	46	144	92	37	71
Миранда Медиа	42	80	19	44	35	15	43	51	141	71	54	89
AvaNet	35	70	17	49	36	15	38	67	168	82	39	85
Полтавка	39	15	17	43	35	17	35	54	148	80	37	76
Бытрадио	36	15	42	38	34	14	34	48	147	68	23	88
КСТ	-	43	16	42	34	17	33	56	156	73	38	84
FarLine	38	66	18	44	34	14	34	53	154	71	118	61
FarLine 2 канал	34	49	14	39	33	13	34	52	150	69	31	106
Викс (Алушта)	37	57	16	46	35	15	37	51	149	99	36	79
Crelcom	37	68	19	39	32	16	33	54	149	85	37	101
Укртелеком ОГО	86	118	67	390	100	69	89	110	201	116	83	134
Укртелеком ОГО 2 канал	62	91	41	65	59	41	60	77	179	105	60	93
Луговое	34	48	15	40	34	67	31	50	151	78	37	75
GigaNet	33	14	14	39	33	14	33	61	144	76	33	74

Таблица 2 – Количество шагов для достижения удаленных серверов

	www.yandex.ru	www.google.com	meta.ua	vk.com	odnoklassniki.ru	www.youtube.com	mail.ru	wikipedia.org	facebook.com	www.avito.ru	www.gismeteo.ru	slando.ua
FreeNet	9	9	7	9	8	6	8	8	18	12	9	12
FreeNet 2 канал	7	9	7	8	8	6	8	9	19	13	12	14
Воля	8	8	8	11	9	7	8	15	18	13	7	15
Ардинвест	13	11	11	14	12	10	12	11	21	19	12	14
Ардинвест 2 канал	11	13	11	13	12	-	12	11	13	19	12	14
Ардинвест 3 канал	12	11	11	14	12	10	11	11	21	19	12	17
Миранда Медиа	7	10	7	9	8	6	7	6	16	14	14	9
AvaNet	9	9	8	10	9	7	9	7	16	11	8	11
Полтавка	10	7	8	11	9	7	8	8	18	16	9	11
Бытрадио	8	7	7	9	8	6	8	8	18	16	8	11
КСТ	-	7	6	9	7	6	6	6	16	14	7	10
FarLine	7	7	8	9	8	6	7	7	18	11	7	12
FarLine 2 канал	7	9	8	8	8	6	8	7	17	11	7	12
Викс (Алушта)	9	10	8	10	9	7	7	6	16	14	14	9
Crelcom	6	8	6	9	7	5	6	6	16	14	7	9
Укртелеком ОГО	7	9	7	9	11	6	8	9	14	11	7	8
Укртелеком ОГО 2 канал	7	9	7	8	7	6	7	9	14	11	7	10
Луговое	7	6	6	8	7	8	7	6	16	14	7	9
GigaNet	7	5	7	10	8	5	7	7	17	15	8	10

По данным, полученным в результате трассировки широко распространенных ресурсов сети Интернет, были построены приблизительные пути передачи информации (рис.1).

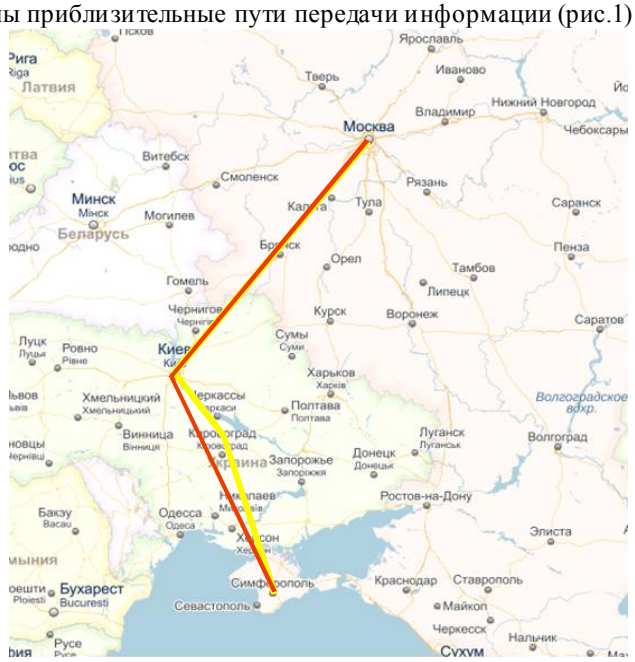

Рисунок 1 – Основные маршруты передачи данных

Из рисунка 1 видно, что, несмотря на расположение удаленных целевых серверов в России, трафик передается через Украину. Поэтому является актуальным подготовка решений по прозрачному переходу на российские магистральные линии связи с целью обеспечения национальной информационной безопасности и построения единой сетевой инфраструктуры государственных учреждений.

Заключение. В ходе проделанной работы проведен системный анализ методов мониторинга сетевого трафика в сетях Интернет-провайдеров. Анализ показал, что каждый из перечисленных методов может быть использован для решения своего круга задач. Для анализа трафика Интернет-провайдеров Крыма на первой стадии с целью выявления путей следования информационных потоков был применен метод трассировки каналов. Получена статистика о маршрутах на наиболее популярный в исследуемом регионе Интернет ресурсы. Выявлена высокая задержка у большинства провайдеров, связанная с тем, что трафик идет не оптимальным путем. Карта маршрутов позволила установить тот факт, что у большинства провайдеров каналы даже на Москву проходят все еще по территории Украины, что может снижать отказоустойчивость сети и нарушает целостность ITинфраструктуры Российской Федерации.

Дальнейшее решение задачи повышения эффективности управления трафиком Интернет-провайдеров Крыма предполагает детальный анализ потоков информации с применением методик опроса SNMP-агентов и, в дальнейшем, анализ типа запросов и протоколов с использованием методики сниффинга.

Библиографический список использованной литературы

1. О применении интеллектуальных технологий в мониторинге компьютерных сетей / Р.Г. Шыхалиев // Искусственный интеллект. — 2011. — № 1. — С. 124-132.

2.Костромицкий А.И., Волотка В.С. Обзор программ анализа и мониторинга сетевого трафика. – Радиотехника. Всеукр. межвед. науч.-техн. сб. – 2010. Вып.162, с. 116-122.

3.Richard A Steenbergen A Practical Guide to (Correctly) Troubleshooting with Traceroute [Электрнный ресурс] NANOG 47, October 18-21, 2009 URL: http://www.nanog.org/meetings/nanog47/presentations/ Sunday/RAS_Traceroute_N47_Sun.pdf (дата обращения: 07.12.2014).

4. Ю.В. Маркин, А.С. Санаров. Обзор современных инструментов анализа сетевого трафика: Препринт 27, ИСП РАН, 2014. – 24с.

Милюков В.В., Зуев С.А., Покрова С.В. Системно-функциональный анализ потоков данных в сетях Интернет-провайдеров Крыма.

В работе рассмотрены базовые методы системного и функционального анализа сетевого трафика, позволяющие получить статистические данные для разработки методик оптимизации и управления качеством обслуживания в мультисервисных сетях. Выполнен системный анализ маршрутов передачи данных провайдеров Крыма и получены их функциональные характеристики. Исследование выполнено

при финансовой поддержке РФФИ в рамках научного проекта № 14-41-01564 «Разработка моделей и методов вероятностного анализа сетевого трафика в условиях гетерогенных потоков данных»

Ключевые слова: потоки данных, сетевые анализаторы, анализ трафика

Milyukov V.V., Zuev S.A., Pokrova S.V. Systemic-functional analysis of the data flow across the Internet service providers in the Crimea.

The system approach of network traffic analysis are discussed in this article. Obtained statistical data to optimize and improve the quality of service in multiservice networks. Tested routes and obtained comparative characteristics data of time delays in the Crimea providers. The reported study was partially supported by RFBR, research project No. 14-41-01564.

Keywords: Data streams, network analyzers, traffic analysis

УДК 621.38

Сосновский Ю.В., доц., канд. техн. наук
Таврический национальный университет им. В.И. Вернадского, Республика Крым г.Симферополь, пр. Вернадского 4.
e-mail: mailsender256@mail.ru

ПРОБЛЕМАТИКА ИДЕНТИФИКАЦИИ ПОТОКОВ ГЕТЕРОГЕННОГО ТРАФИКА В УСЛОВИЯХ НЕСТАЦИОНАРНОСТИ[18]

Статья содержит обзор фундаментальных исследований в области анализа сетевого гетерогенного трафика в условиях нестационарности.

Ключевые слова: *анализ сетевого трафика, гетерогенность, нестационарность*

Проблема идентификации потоков гетерогенного трафика сама по себе является достаточно сложной научной задачей. Гетерогенность сетевого трафика проявляется в наличии в составе передаваемых блоков данных различных компонент трафика, например HTTP-трафика, потокового видео и аудио, а также шифрованного трафика, который имеет измененный профиль за счет перепаковки исходных пакетов того или иного протокола. Гетерогенность трафика отмечена достаточно давно, например в [1].

В отчете 2014 года, опубликованным Sandvine (http://www.sandvine.com/trends/global-internet-phenomena), указывается по сравнению с прошлым годом, в 2014 году отмечено увеличение доли зашифрованного трафика. Лидером роста является Европа (процент зашифрованного интернет-трафика в периоды пикового времени увеличился за год с 1,47% до 6,10%). Средний показатель роста абсолютного интернет-трафика увеличивается на 20%-40% за год, в тоже время пропускная способность каналов, потребляемая зашифрованным трафиком, удваивается в этот период. Аналогичная ситуация наблюдается также в сетях мобильной связи, где зашифрованный трафик также растет. Важно отметить, что значительный рост зашифрованного трафика приходится на SSL-шифрование, что с позиции системного администратора не является неразрешимой проблемой, хотя и привносит существенные трудности в сигнатурный анализ передаваемых данных и значительно снижает эффективность работы сетевых сканеров, работающих по принципам сигнатурного анализа потоков данных.

Ряд источников, как независимые эксперты, так и группы аналитиков [2] отмечают, что около 40% клиентов пиринговых одноранговых сетей (P2P) по тем или иным соображениям используют шифрование трафика. Самые известные представители P2P сетей – торренты, и шифрование не скрывает адрес источника и получателя, но скрывает сам факт передачи именно P2P трафика.

В тоже время отмечен рост популярности VPN-сетей, кроме того ведущие ученые предлагают расширить это понятие и начать переход на новый уровень виртуализации компьютерных сетей [3]. Можно привести множество ссылок на самые современные публикациипо теме роста объемов трафика, генерируемых VPN-сетями, повышением требований к пропускной способности каналов и защищенности такого трафика, однако объем статьи не позволяет этого сделать.

Несколько обособленно находится т.н. анонимная сеть виртуальных туннелей Tor, осуществляющая передачу данных в зашифрованном виде и позволяющая пользователю сохранять анонимность в Интернет. Ввиду высокой степени анонимности существует значительное число свидетельств использования данной технологии для распространения вредоносных программ, вирусных атак и т.п.[4,5]. При этом отмечается, что сама по себе идентификация подобного шифрованного трафика уже представляет собой серьёзную проблему, особенно в условиях общего гетерогенного потока, генерируемого различными системами, приложениями и сервисами. Еще боле сложной задачей в этих

[18] Работа выполнена при финансовой поддержке РФФИ (грант № 14-41-01564).