# Введение

**Актуальность области исследования**. В наши дни производительность сетей передачи данных достигла показателей, позволяющих передавать аудио- и видеоданные реального времени. Количество таких сервисов неумолимо растет и все больше операторов связи предоставляют такие услуги своим клиентам. В связи с валовым ростом интереса к получению данных услуг, актуальной становится задача адекватной оценки предоставляемого провайдером сервиса. Эта задача особенно актуальна в случае предоставления мультимедийного сервиса реального времени, который в значительной степени чувствителен к задержкам передачи трафика.

Необходимо отметить, что к настоящему времени теория оценки параметров качества предоставляемого мультимедийного сервиса в пакетных сетях недостаточно развита. Некоторые критические параметры состояния сети, такие как, например, вариация задержки в канала, не имеют однозначного способа оценки, что говорит об актуальности области исследования.

**Объектом исследования** являются известные методы подсчета вариации задержки в компьютерных сетях при передаче голосового и видеотрафика.

**Предметом** исследования является изучение влияния выбора методики расчёта вариации задержки на конечные метрики оценки качества канала связи..

**Цель исследования** – провести сравнительный анализ методов расчёта вариации задержки в компьютерных сетях и, на основе проведенного анализа, доказать необходимость стандартизации этих методик.

Для достижения цели исследования решались следующие **задачи**:

1. Выполнить аналитический обзор литературы, посвящённой проблеме расчета реального значения вариации задержки в компьютерных сетях.
2. Собрать репрезентативные данные о задержках в компьютерных сетях для дальнейших расчетов вариации задержки по выявленным методикам.
3. Провести расчет вариации задержки на основе полученных данных о задержках в компьютерных сетях.
4. Сравнить полученные результаты расчётов.
5. Проанализировав результаты сделать выводы о применимости методов расчета вариации задержки и, возможно, о необходимости их стандартизации.

**Теоретическая и методологическая основа исследования. При** Перечисляются использованные методы и средства исследовании, а также применяемые в работе инструменты исследования: аппарат теории вероятностей, теории массового обслуживания (ТМО), теории случайных процессов, теории планирования машинного эксперимента, методы численного анализа и имитационного моделирования, а также даётся перечень использованных инструментов, например: название IDE, типы СУБД, языки программирования, библиотеки, математическое ПО (Matlab, Mathcad, Octave, R,…) и т.п. (1-2 абзаца). Если тяжело наскрести хотя бы два пункта, можно подобрать что-нибудь из следующего списка: метод обобщений, формально-логический метод, структурно-функциональный анализ, общенаучный метод абстрагирования, метод сравнений и аналогий, метод перехода от общего к частному, от абстрактного к конкретному, от идеального к материальному.

**Актуальность темы исследования.** Здесь нужно обосновать не актуальность области исследования (как было в начале ВВЕДЕНИЯ), а актуальность конкретной выбранной темы исследования. Например, для темы ВКР «Повышение плотности записи информации на перфокартах» очень просто обосновать актуальность области исследования, т.к. область связана с развитием систем хранения данных, что на данный момент очень актуально. Однако обосновать актуальность такой темы исследования будет очень сложно, ведь перфокарты уже давно не используются (1 абзац).

**Степень теоретической разработанности темы**. Описывается степень проработанности темы другими авторами и краткая история развития тематики. Перечислить наиболее авторитетных за последние 10 лет авторов книг или авторов диссертаций (кандидатских и докторских) на выбранную или схожую тему (1 абзац).

**Информационная база исследования**. Написать, на какие конкретно труды и материалы в первую очередь опирался автор ВКР, например: книги, статьи, отчёты, доклады, статистические материалы, исследовательские сайты, репозитории, нормативные акты (законы, кодексы). В отличие от предыдущего, в этом пункте нужно не просто назвать авторов, а указать названия конкретных работ, которые использовались в качестве основы в ВКР (1 абзац).

**Научная новизна исследования.** Показать, что именно сделал автор, чего раньше никто не делал ... (2-3 абзаца).

**Практическая значимость исследования**. Указать, кому, в каком виде и в каких именно областях в практическом смысле пригодятся результаты, полученные автором в ВКР (1 абзац).

**Апробация результатов исследования**. Указать, используются ли где-нибудь на практике полученные в ВКР результаты. Перечислить конференции, на которых делались доклады по теме ВКР. Указать количество опубликованных работ (при наличии) – список названий публикаций писать не надо, его надо поместить в общий список литературы, а здесь просто поставить ссылку в квадратных скобках (1 абзац).

**Объем и структура работы**. Указать краткое содержание каждой главы: по одному длинному предложению на каждую главу. Предложения должны начинаться: «В первой главе раскрывается/описывается/приводится…» (1 абз.).

**ГЛАВА 1.**

**1.1 История развития области исследования.**

История сетей коммуникации насчитывает более полутора веков, начиная свой отсчет с изобретения телеграфа. С тех пор технологии значительно шагнули далеко вперед. Структура сети полностью менялась с приходом новых технологий.

Более ста лет назад, телефонные сети общего пользования начали формировать всемирную сеть с коммутацией каналов. Полоса пропускания такой сети была фиксированной, что идеально подходило для передачи трафика реального времени, такого как голос.

Спустя 50 лет, специалисты представили миру сеть с коммутацией пакетов. Такая сеть позволяла делить поток данных на отдельные порции и отправлять их в пункт назначения различными путями.

Появление IP Quality of Service не было неожиданностью. Еще отцы основатели Интернета предвидели его необходимость и включили поле Type of Service в заголовок IP-пакета для дальнейшего облегчения внедрения QoS. Спецификация протокла IP описывает поле ToS, как индикатор желаемого качества обслуживания. Этот параметр используется для выбора параметров передачи датаграммы через ту или иную сеть.

В конце 80х годов 20го века Интернет использовался лишь в академических и военных целях, что означало ограниченное количество передаваемых через него данных. Поэтому в поле ToS не было необходимости, и почти все реализации протокла IP игнорировали его. При отправке пакета это поле оставалось пустым, а маршрутизаторы не использовали его при выборе дальнейшего маршрута до пункта назначения.

Необходимость в QoS для сети Интернет возрастала с ее выходом из академической среды в более широкое использование в коммерческих и частных целях. Для передачи данных в Интернет используется стек TCP/IP, что делает его гибким и надежным. Но несмотря на это, сеть подвержена перегрузкам. Чаще всего в роли так нзываемого «бутылочного горлышка» выступают маршрутизаторы, соединяющие две сети с различной пропускной способностью. Этой проблемой заинтересовался Джон Нейгл в середине 80х годов.

Документ Нейгла, Управление Перегрузкой IP/TCP Сетей (RFC 896) описывает то, что он назвал «проблемой небольших пакетов», которая заключается в том, что приложение неоднократно посылает данные небольшими порциями, часто размером в 1 байт. Так как TCP пакеты имеют 40 байт заголовка (20 байт TCP, 20 байт IPv4), это приводит к тому, что передается пакет размером 41 байт, несущий в себе 1 байт полезной информации, то есть к огромным накладным расходам. Эта ситуация часто встречается в сессии Telnet, где большинство нажатий клавиш генерируют один байт данных, который немедленно передается. Кроме того, по медленным каналам связи многие такие пакеты могут находиться в пути в одно и то же время, что может привести к перегруженности сети.

Алгоритм Нейгла работает путём объединения нескольких небольших исходящих сообщений, а затем отправки их всех сразу. В частности, пока существует отправленный пакет, для которого отправитель еще не получил никакого подтверждения о доставке, отправитель должен держать в буфере следующие данные для отправки, до тех пор, пока не наберется достаточно данных на полный пакет, который можно отправить единожды. Данный алгоритм считается первой вехой в истории QoS.

В 1986 году американский ученый Ван Якобсон разработал новый набор инструментов QoS — механизмы предотвращения перегрузок, которые по сей день используются в реализации протокола TCP. Этими механизмами являются медленный старт и алгоритм контроля перегрузок, которые помогли сети Интернет избежать коллапса при значительном росте трафика в 1988—1989 годы. Еще два механизма, быстрая повторная передача и быстрое восстановление, были добавлены для обеспечения более высокой производительности при потере пакетов.

Несмотря на то, что описанные выше механизмы в значительной мере увеличивали производительность сети, оставалась проблема перегрузок при маршрутизации. Именно поэтому в 1990 году внимание исследователей было сконцентрировано вокруг маршрутизаторов. Когда передача данных сталкивается с проблемой «бутылочного горлышка» для приёма и отправки пакетов на маршрутизаторах, то обычно используется метод FIFO: первый пришел - первый ушёл (First In — First Out). При интенсивном трафике это создаёт заторы, которые разрешаются крайне простым образом: все пакеты, не вошедшие в буфер очереди FIFO (на вход или на выход), игнорируются маршрутизатором и, соответственно, теряются безвозвратно. Алгоритмы взвешенной справедливой очереди и взвешенного произвольного раннего обнаружения были разработаны для решения этой проблемы.

Следующим этапом развития стало изобретение сквозного (на всём пути следования трафика) качества обслуживания. Архитектура Intserv, разработанная инженерным советом Интернета, была призвана предоставить средства для передачи в сеть своих требований к качеству обслуживания трафика. С целью сообщения маршрутизаторам сети потребностей конечных узлов по качеству обслуживания потоков был разработан дополнительный протокол — RSVP. Хотя в середине 90-х годов прошлого века идея IntServ и RSVP вызывала большие надежды, со временем интерес к этой архитектуре угас. Главной причиной стала проблема масштабируемости, вызванная необходимостью хранить и поддерживать информацию о состоянии передачи в каждом маршрутизаторе. Эта проблема, переносимая на такие глобальные сети, как Интернет, отдаляет RSVP от реальности.

Одной из последних вех в QoS является внедрение модели DiffServ. Дифференцированое обслуживание предполагает разделение трафика на классы на основе требований к качеству обслуживания. Каждый класс трафика дифференцируется и обрабатывается сетью в соответствии с заданными для этого класса механизмами QoS. Подобная схема обеспечения качества обслуживания (QoS) довольно часто называется схемой CoS.

Архитектура DiffServ подразумевает определение поля DiffServ (DS), которое заменяет поле типа обслуживания в протоколе IPv4, используемое при принятии решений о пересылке данных через каждый узел для классификации пакетов и функций согласования трафика, например таких, как измерение, маркирование, формирование и контроль.

Стандарты RFC не устанавливают метода реализации пересылок данных через каждый узел, перенося всю ответственность за это на производителя оборудования. Компания Cisco реализует технологию организации постановки в очередь, которая может основывать пересылку данных через каждый узел на базе IP-приоритетов или значений кода DSCP в заголовке IP-пакета. Основываясь на коде DSCP или IP-приоритете, трафик может быть вставлен в определенный класс обслуживания. Пакеты в рамках какого-либо класса обслуживания обрабатываются одинаково.

Дифференцированное обслуживание удобно применять в сетях с интенсивным

трафиком приложений. В этом случае важно обеспечить отделение административного трафика сети от всего остального трафика и назначить ему приоритет, позволяющий в любой момент времени быть уверенным в связности узлов сети.

**1.2. Основные характеристики канала связи**

Внедрение механизмов QoS предполагает обеспечение со стороны сети соединения с определенными ограничениями по производительности. Основными характеристиками производительности сетевого соединения являются полоса пропускания, задержка, вариация задержки и уровень потери пакетов.

**1.2.1 Полоса пропускания**

Термин полоса пропускания (bandwidth) используется для описания номинальной пропускной способности среды передачи информации, протокола или соединения. Этот термин достаточно эффективно определяет “ширину канала”, требующуюся приложению для взаимодействия по сети. Как правило, каждое соединение, нуждающееся в гарантированном качестве обслуживания, требует от сети резервирования минимальной полосы пропускания. К примеру, приложения, ориентированные на передачу оцифрованной речи, создают поток информации интенсивностью 64 Кбит/с. Эффективное использование таких приложений становится практически невозможным вследствие снижения полосы пропускания ниже 64 Кбит/с на каком-либо из участков соединения.

**1.2.2 Потеря пакетов**

Уровень потери пакетов (packet loss) определяет количество пакетов, отбрасываемых сетью во время передачи. Основными причинами потери пакетов являются перегрузка сети и повреждение пакетов во время передачи по линии связи. Чаще всего отбрасывание пакетов происходит в местах перегрузки, где число поступающих пакетов намного превышает верхнюю границу размера выходной очереди. Кроме того, отбрасывание пакетов может быть вызвано недостаточным размером входного буфера.

Как правило, уровень потери пакетов выражается как доля отброшенных пакетов за определенный интервал времени.

**1.2.3 Задержка и джиттер при передаче пакетов**

Задержка при передаче пакета (packet delay), или латентность (latency), на каждом переходе состоит из задержки сериализации, задержки распространения и задержки коммутации. Ниже приведены определения каждого из названных выше типов задержки.

1. Задержка сериализации (serialization delay). Время, которое требуется устройству на передачу пакета при заданной ширине полосы пропускания. Задержка сериализации зависит как от ширины полосы пропускания канала передачи информации, так и от размера передаваемого пакета. Например, передача пакета размером 64 байт при заданной полосе пропускания 3 Мбит/с занимает всего лишь 171 нс. Обратите внимание, что задержка сериализации очень сильно зависит от полосы пропускания: передача того же самого пакета размером 64 байт при заданной полосе пропускания 19.2 Кбит/с занимает уже 26 мс. Довольно часто задержку сериализации называют еще задержкой передачи (transmission delay).
2. Задержка распространения (propagation delay). Время, которое требуется пере-анному биту информации для достижения принимающего устройства на другом конце канала. Эта величина довольно существенна, поскольку в наилучшем случае скорость передачи информации соизмерима со скоростью света. Обратите внимание, что задержка распространения зависит от расстояния и используемой среды передачи информации, а не от полосы пропускания. Для линий связи глобальных сетей задержка распространения измеряется в миллисекундах. Для трансконтинентальных сетей Соединенных Штатов характерна задержка распространения порядка 30 мс.
3. Задержка коммутации (switching delay). Время, которое требуется устройству, получившему пакет, для начала его передачи следующему устройству. Как правило, это значение меньше 10 нс. Обычно каждый из пакетов, принадлежащий одному и тому же потоку трафика, передается с различным значением задержки. Задержка при передаче пакетов меняется в зависимости от состояния промежуточных сетей.

В том случае, если сеть не испытывает перегрузки, пакеты не ставятся в очередь в маршрутизаторах, а общее время задержки при передаче пакета состоит из суммы задержки сериализации и задержки распространения на каждом промежуточном переходе. В этом случае можно говорить о минимально возможной задержке при передаче пакетов через заданную сеть. Следует отметить, что задержка сериализации становится незначительной по сравнению с задержкой распространения при передаче пакета по каналу с большой пропускной способностью. Если же сеть перегружена, задержки при организации очередей в маршрутизаторах начинают влиять на общую задержку при передаче пакетов и приводят к возникновению разницы в задержке при передаче различных пакетов одного и того же потока. Изменение задержки при передаче пакетов получило название джиттера (packet jitter). Джиттер имеет большую важность, поскольку именно он определяет максимальную задержку при приеме пакетов в конечном пункте назначения. Принимающая сторона, в зависимости от типа используемого приложения, может попытаться компенсировать вариацию задержки за счет организации приемного буфера для хранения принятых пакетов на время, меньшее или равное верхней границе джиттера.

К этой категории относятся приложения, ориентированные на передачу/прием непрерывных потоков данных, например Internet-телефония или приложения, обеспечивающие проведение видеоконференций.

Причиной джиттера могут быть разные факторы, обусловленные спецификой передачи информации в пакетных сетях: это и большая загрузка узлов коммутации, где пакеты выстраиваются в очередь и ожидают своей отправки в следующую точку агрегации и маршрутизации сетевого трафика, это и диверсификация маршрутов следования пакетов (пакеты, следовавшие друг за другом в источнике, могут быть переданы разными маршрутами к получателю, а значит, и вероятно обработаны разным количеством сетевых узлов, каждый из которых вносит свою, случайную задержу обработки пакета).

**1.3 Методы расчета вариации задержки**

При заключении договора на предоставление услуг связи между поставщиком и клиентом заключается договор SLA(Service Level Agreement), в котором явно указывается то качество услуг, которое поставщик обязан предоставить потребителю. Не последнюю роль в данном соглашении играют метрики QoS, в том числе и вариация задержки. В документе RFC5481 упоминается, что обычно требования к джиттеру формулируются в виде количества пакетов имеющих джиттер не больший, чем установлено соглашением на определённом промежутке времени. Однако, существует множество методов расчёта вариации задержки, которые будут рассмотрены в следующем пункте.

**1.3.1. Inter-Packet Delay Variation**

Самым простым известным методом измерения джиттера является метод измерения вариации задержки между двумя следующими друг за другом пакетами.

IPDV(i) = Delay(i) – Delay(i-1),

где Delay(i) – односторонняя задержка пакета, для которого производится измерение, а Delay(i-1) – задержка при передаче предыдущего пакета.

Значения IPDV могут быть как положительными, так и отрицательными, но несмотря на это принято брать абсолютное значение.

**1.3.2 Packet Delay Variation**

Термин Packet Delay Variation (PDV) впервые был определен в документе Y.1540 : Internet protocol data communication service - IP packet transfer and availability performance parameters. Эти термином обозначается разница задержек пакета, для которого производится расчёт, и минимальной задержки пакета на всем интервале измерений.

PDV рассчитывается для пары, где одним из пакетов является пакет, для которого происходит вычисление, а вторым является так называемый эталонный пакет.

PDV(i) = Delay(i) – Delay(ref),

В Y.1540 приводится несколько способов выбора эталонного значения задержки:

* минимальная задержка;
* средняя задержка на всем интервале измерения;
* задержка при передаче первого пакета.

**1.3.3.Рассчет джиттера в протоколе RTP**

RTP – протокол передачи данных реального времени. Данный протокол широко используется для передачи аудио- и видеотрафика в таких программных продуктах, как, например, Astesisk. На практике протокол RTP не отделим от протокола RTCP (RTP control protocol). Последний служит для мониторинга QoS и для передачи информации об участниках обмена в ходе сессии. [RFC1889].

Протокол RTCP так же содержит в себе механизм расчета вариации задержки. Джиттер рассчитывается на основании предыдущего значения и настоящего значения задержки пакета.

Джиттер *Ji* для *i*-го пакета определяется по формуле:

где:

– отклонение от ожидаемого времени прибытия i-го пакета.

Отклонение от ожидаемого времени прибытия i-го пакета определяется по формуле:

, где:

R – время прибытия пакета в метках времени RTP,

*S* – временная метка RTP, взятая из пакета.

**1.4. Выводы по главе**

1. История области исследования берет начало в 80х годах прошлого века и до сих пор актуальна.
2. Среди всех метрик QoS вариация задержки является особо важной при передаче трафика реального времени.
3. На данный момент существует 5 методов расчёта джиттера и не имеется единого стандарта, на который можно опираться при описании качества предоставляемых поставщиком услуг передачи данных.

**Глава 2. Описение метода сбора данных сетевых задержек и рассчета вариации задержки различными методами**

Для достижения целей выпускной квалификационной работы был разработан стенд по расчету вариации задержки различными методами, который берез в качестве входных данных реальные значения задержек, измеренные при помощи инструмента Scamper.

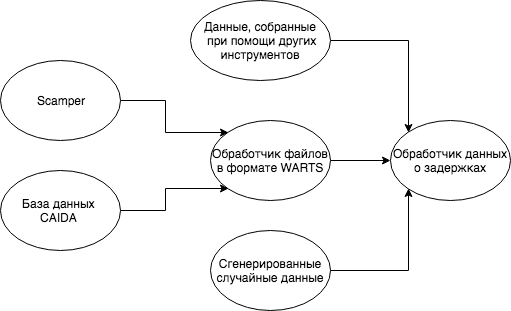


Рисунок \* - Схема экспериментального стенда

Данные о задержках можно либо собирать при помощи утилиты Scamper, либо взять дампы данных в формате warts с открытого сайта научной организации CAIDA. Далее warts файлы поступают на обработку скрипта на языке Python, который генерирует файл, содержащий только значения задержек, по одному значению в каждой строке. Затем запускается скрипт на языке R, который производит расчеты вариации задержки различными методами и их сравнение.

* 1. **Структура компонентов эксперементального стенда**

2.1.1. Орагнизация по исследованию Интернета CAIDA

Center for Applied Internet Data Analysis (CAIDA) – научная организация, основанная в 1997 году, которая проводит исследование состояния компьютерных сетей и строит исследовательскую инфраструктуру для сбора данных и распространения их в научной среде. Исследовательская группа, расположенная в федеральном центре суперкомпьютеров Сан-Диего, проектирует, разворачивает и поддерживает растущее количество сервисов для вычислений, анализа и визуализации данных. Так же исследовательская группа распространяет измерительную аппаратуру и внедряет ее в сети по всему мир. Исследователи CAIDA разрабатывают новые технологии сбора, анализа и визуализации получаемых данных.

CAIDA исследует теоретические и практические аспекты работы Интернета:

* формирование понимая глобальных функций инфраструктуры глобальной сети, ее поведения, использования и эволюции;
* способствование созданию совместной инфраструктуры для распространения и анализа научных данных;
* создание целостного представления о науке об Интернете;
* информирование исследователей, производителей и законодателей в сфере информационных технологий о проблемах глобальной сети.

Исследование, проводимое CAIDA, охватывает топологию, маршрутизацию, безопасность и экономику Интернета. Деятельность CAIDA по разработке программного и аппаратного обеспечения и распространению информации обеспечивает данными не только исследовательский центр университета Сан-Диего, но и ученых по всему миру.

Так же, CAIDA занимается картографией Интернета, составляя карту глобальной сети, используя при этом свою инфраструктуру. Основной задачей является улучшение точности и поддержание карты в актуальном состоянии. Так же исследовательской группой совместно с учеными из Массачусетского Технологического Института ведется работа по нанесению на карту всех соединений между различными провайдерами услуг связи, для исследования перегрузок, вызванных пирингом и работой сервисов CDN.

CAIDA проводит мониторинг безопасности и стабильности глобальной сети и имеет свою открытую базу данных, которые могут быть свободно использованы для исследователями процессов, происходящих в глобальной сети, учеными со всего мира. Так же CAIDA разрабатывает множество инструментов для сбора или анализа таких данных.

* + 1. **Утилита Scamper**

Scamper – это инструмент сбора данных о состоянии сети для дальнейшего анализа ее топологии и производительности. Данное программное обеспечение было разработано программистом из Новой Зеландии Мэттью Лаки для CAIDA при участии ученых из Открытого Центра Инноваций Университета Ваикато и активно используется начиная с сентября 2008 года. Уже к августу 2010 года было активно 48 точек по всему миру под управлением трех команд, из которых производились замеры. Данное программное обеспечение распространяется по стандартной общественной лицензии GNU GPL v2+. В отличие от его предшественника skitter, он позволяет зондирование, как IPv4 адресов, так и IPv6. Данный инструмент позволяет производить измерения множеством методов:

* Traceroute
* Ping
* MDA traceroute
* Alias resolution
* Sting
* TBIT

Изначально scamper был разработан для сбора данных о производительности сетей в рамках проекта исследовательской группы CAIDA для изучения глобальной топологии сети Интернет. Трассировка пакетов в scamper имеет множество функций: она поддерживает обе версии сетевого протокола IP (четвертую и шестую); измерения могут производиться при помощи трех протоколов канального уровня: UDP, TCP и ICMP, такое разнообразие протоколов позволяет получать данные практически из любой конечной точки в большинстве автономных систем.

Метод Ping позволяет измерять сквозные задержки и потерю пакетов при передаче по сети, определять доступность IP адресов и классифицировать поведение хостов, оценивая их ответы на запросы. В дополнение к традиционному методу эхо-запросов по протоколу ICMP, scamper реализует так же измерение посредством UDP, TCP и TTL-limited запросов, которые могут быть использованы в случае, если обычные ICMP запросы остаются без ответа.

Помимо упомянутых выше способов scamper реализует многопутевой алгоритм детектирования, позволяющий определить все интерфейсы на всех возможных путях следования пакета от источника до пункта назначения. Это достигается путем умышленного варьирования идентификатора потока, который маршрутизатор может рассчитывать при балансировке нагрузки. Запросы с разными идентификаторами могут быть отправлены разными маршрутами, тем самыми выявить все узлы, через которые можно достичь пункта назначения. В дополнение к стандартным методам варьирования контрольных сумм ICMP и портов назначения в UDP, в scamper так же реализован метод изменения исходящего порта, что позволяет обходить некоторые сетевые экраны, которые могут блокировать запросы, принимая их за сканирование портов злоумышленниками.

Alias resolution – это метод трассировки, позволяющий определить связи между интерфейсами маршрутизаторов. Данный метод позволяет определить адреса интерфейсов, принадлежащих одному маршрутизатору, данная информация является ключевой при построении карты топологии Интернета.

Scamper позволяет получать выходные данные двух видов: обычный текстовый формат в кодировке ASCII и бинарный. Данные в текстовом виде имеют формат, сходный с выводом стандартных утилит ping и traceroute, и удобны для использования scamper в интерактивном режиме. Бинарный вид удобен для использования исследователями сети, благодаря возможности получения большего количества деталей и удобству хранения в файлах формата warts [warts]. Scamper включает в себя библиотеку для обработки бинарных данных именно в этом формате, а так же, участниками CAIDA была разработана библиотека для языка Ruby, позволяющая писать на нем программы для анализа выходных данных. Так же scamper предоставляет API для реализации новых методов сбора данных и сохранения их в бинарном формате. Библиотека не поддерживает функцию чтения данных из текстового файла, это было сделано намерено, чтобы заставить разработчиков отказаться от использования текстового формата и поощрить использование бинарного.

Пакет scamper включает множество утилит:

* scamper: основная утилита для сбора данных,
* sc\_analysis\_dump: утилита для конвертации данных в формат, удобный для обработки на языке Perl,
* sc\_filterpolicy: драйвер для исследования систем на предмет соответствия политикам фильтрации,
* sc\_remoted: утилита для подключения и сбора данных с удаленных сборщиков данных,
* sc\_tbitblind: драйвер для исследования систем на предмет уязвимости к атаке «слепой подмены»,
* sc\_tbitpmtud: драйвер для исследования систем на предмет чувствительности к слишком большим ICMP пакетам,
* sc\_tracediff: утилита для отслеживания изменений маршрутизации в сети,
* sc\_warts2csv: утилита для конвертации warts фалов в формат csv,
* sc\_warts2json: утилита для конвертации warts файлов в формат JSON,
* sc\_warts2pcap: утилита для конвертации warts файлов в формат pcap,
* sc\_warts2text: утилита для конвертации warts файлов в обычный текстовый формат.
* sc\_wartscat: утилита для конкатенации нескольких файлов в формате warts
* sc\_wartsfix: утилита для восстановления поврежденных файлов в формате warts.
  + 1. **Конвертация warts файлов**

Для расчета вариации задержки необходимо получить данные о задержках при передаче пакетов. Так как основной скрипт-обработчик, который производит расчет вариации задержки различными методами, принимает на вход текстовые файлы, в которых каждое значение задержки располагается на отдельной строке, необходимо привести все данные к этому формату. Для эти целей был разработан скрипт warts\_converter.py на языке Python версии 2.7. В качестве аргумента скрипт принимает путь до папки с warts-файлами. Помимо базовых модулей в скрипте используются python-модули os, sys и scamper-pywarts[pywarts].

Модуль os в Python предназначен для взаимодействия программы с операционной системой, в частности, для управления файлами. Иногда нужно автоматизировать какие-то действия с файлами, например, создать автоматический установщик, или программу, делающую бэкап документов на второй раздел диска. В данном скрипте, модуль os используется для операций с путями файлов, получения имен файлов, расположенных в папке, и создания новых папок на файловой системе.

Модуль sys содержит информацию о среде выполнения программы, об интерпретаторе Python. В скрипте-конвертере использование данного модуля обусловлено необходимостью получения параметров запуска скрипта, а именно папки, в которой находятся файлы в формате warts, которые будут подвергаться конвертации.

Модуль scamper-pywarts – это библиотека с открытым исходным кодом на языке Python, предназначенная для чтения и обработке файлов в формате warts. Данный модуль просто в использовании и имеет множество достоинств:

* реализация на чистом языке Python, отсутствие зависимостей;
* поддерживает обе версии языка Python;
* легко расширяемый, благодаря открытости исходного кода;
* обладает высокой производительностью (для обработки warts-файла, содержащего данные трассировок, размером 80 мегабайт необходимо меньше минуты);
* реализует потоковую обработку данных, так как единовременно в памяти находится только одна запись. Это позволяет обрабатывать большие warts-файлы при ограниченном ресурсе виртуальной памяти и получать данные напрямую на выходе утилиты scamper.

В качестве аргумента данный скрипт принимает путь до директории с warts файлами и приводит все файлы в ней к виду,

* + 1. Программа расчета вариации задержки различными методами

Программа обработки данных и расчета вариации задержки была реализована при помощи математического пакета R.

R - язык программирования для статистической обработки данных и работы с графикой, но в тоже время это свободная программная среда с открытым исходным кодом, развиваемая в рамках проекта GNU. Среда программрования R поставляется в большинстве дистрибутивов GNU/Linux и находит свое применение везде при работу с данными. Это не только статистика в узком смысле слова, но и «первичный» анализ (графики, таблицы сопряжённости), и продвинутое математическое моделирование. Среда R так же может послужить бесплатной заменой популярным коммерческим пакетам, таким как Octave и MatLab. С другой стороны, вполне естественно, что основная вычислительная мощь R лучше всего его проявляется при статистическом анализе: от вычисления средних величин до вейвлет-преобразований временных рядов.

**Бибилиографический список**

[warts] - <https://www.caida.org/tools/measurement/scamper/man/warts.5.pdf>

[pywarts] - https://pypi.org/project/scamper-pywarts/