СТАТИСТИЧЕСКАЯ ОЦЕНКА ЛОКАЛЬНОЙ КОРРЕКЦИИ СЕТЕВОЙ ДЕГРАДАЦИИ В ЛАБОРАТОРНОЙ СЕТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Исаев Н.А.[1]

Ключевые слова: *сетевая наблюдаемость, сетевые метрики, доверительные интервалы, критерий Стьюдента, UDP-потоки, интегральный критерий качества режима, адресная коррекция, интегральный критерий качества режима, физическая топология сети.*

Аннотация

Цель статьи. *Разработать и проверить подход, позволяющий оценивать, как локальное изменение сетевой обработки влияет на совокупное состояние лабораторной сети, используемой в задачах информационной безопасности. Основная задача состоит в том, чтобы связать ухудшение сетевых показателей с измеряемой причиной и проверить результат коррекции не по одному признаку, а по группе взаимосвязанных метрик.*

Методы исследования. *Работа выполнена на контролируемой сетевой конфигурации из передающего узла, четырёх принимающих узлов, управляемого коммутатора канального уровня и двух логических сегментов трафика. Нагрузка формировалась параллельными однонаправленными потоками протокола пользовательских датаграмм, а измерения проводились на стороне получателей и передающего узла. Сравнивались исходное состояние сети, состояние после расширения наблюдаемости и состояние после адресной коррекции. Для обработки применялись повторные прогоны, средние значения, доверительные интервалы и критерий Стьюдента для связанных выборок.*

Результаты исследования. *Сравнение режимов R_0, R_1 и R_2 показало, что расширение наблюдаемости является диагностическим, но не достаточным корректирующим этапом: оно позволило выявить связь деградации с состоянием очередей, загрузкой узла-источника и признаками сетевой обработки, однако наилучшие значения показателей были получены только после адресной коррекции выявленного участка.*

Наибольший эффект достигается после выявления локального источника деградации и коррекции соответствующего участка сетевой обработки. В измеренной серии уменьшились потери пакетов и задержка, сократилась загрузка передающего узла, увеличилась фактическая скорость приёма данных и стабилизировалось состояние очередей. Интегральная оценка подтвердила согласованное улучшение группы показателей, а не отдельной метрики. Это даёт возможность использовать предложенный подход в области информационной безопасности для экспериментальной диагностики сетевых участков, где необходимо обосновать корректирующее действие до замены оборудования, изменения топологии или снижения заданной нагрузки. В прикладном плане работа показывает, как переход от наблюдения к проверенной коррекции делает сетевой анализ более доказательным.

DOI: 10.24412/1994-1404-2026-2-62-72

Введение

В настоящее время сетевые контуры информационной безопасности обслуживают не только прикладной обмен, но и потоки журналов, телеметрии, событий мониторинга и управляющих сообщений [1, 2]. Рост такого обмена усложняет диагностику: ухудшение может быть связано не с отказом отдельного канала, а с локальной перегрузкой сетевой обработки, которая отражается на нескольких измеряемых характеристиках одновременно. Поэтому требуется методика, позволяющая заранее определить границу эксперимента, выбрать набор сетевых метрик, локализовать источник деградации и статистически проверить результат корректирующих действий.

Цель работы — разработать и проверить методику, позволяющую не только зафиксировать ухудшение сетевых показателей, но и связать его с конкретной причиной в пределах заданной лабораторной границы. Методика включает выбор контролируемых метрик,

[1] ***Исаев Николай Александрович****, аспирант, Московский университет имени С.Ю. Витте, Москва, Россия. ORCID: 0009-0007-3987-1670.*

E-mail: supercopen@yandex.ru

сбор данных по повторным прогонам, анализ очередей и загрузки узла, применение корректирующего действия и статистическую проверку полученного эффекта. Гипотеза исследования состоит в том, что спиральная модель, объединяющая расширенную наблюдаемость и поэтапную коррекцию, позволяет улучшать состояние сети через воздействие на выявленный локальный источник деградации. Предполагается, что изменение одного ключевого участка сетевой обработки способно дать согласованное улучшение пяти показателей: потерь пакетов, фактической скорости приёма данных на стороне получателей, задержки, загрузки передающего узла и состояния очередей.

Научная новизна работы заключается в том, что локальная сетевая деградация оценивается не по отдельному показателю, а по согласованной группе измеряемых характеристик: потерям UDP-пакетов[2], фактической скорости приёма данных на стороне получателей, задержке, загрузке передающего узла и состоянию сетевых очередей. Предложен порядок, при котором сначала задаются границы лабораторного эксперимента, затем фиксируется исходное состояние сети, расширяется наблюдаемость, определяется причина ухудшения и только после этого применяется корректирующее действие. Эффект коррекции проверяется не по одному среднему значению, а по серии повторных измерений с расчётом доверительных интервалов и парным сравнением режимов до и после изменения.

Практическая значимость состоит в том, что предложенный порядок может использоваться для проверки сетевых участков, обслуживающих контуры информационной безопасности. Он позволяет отличить случайное колебание показателей от устойчивого улучшения, определить, связана ли деградация с очередями, нагрузкой узла или служебной конкуренцией, и обосновать корректирующее действие до замены оборудования или изменения топологии.

Постановка задачи и граница эксперимента

Лабораторная сеть в работе рассматривается как контролируемая конфигурация из узлов, управляемого L_2-коммутатора[3], VLAN-сегментов[4] и средств регистрации сетевых показателей. Она используется для воспроизводимого сравнения нескольких состояний одной и той же сетевой конфигурации: исходного состояния без коррекции, состояния с расширенным набором измеряемых признаков и состояния после корректирующих действий. Далее эти состояния обозначаются как R_0, R_1 и R_2.

Граница эксперимента определяется составом элементов, которые участвуют в измерении и не меняются между сравниваемыми состояниями: передающий узел, принимающие узлы, порты коммутатора, прикладной и служебный VLAN-сегменты, а также журналы потерь, задержки, фактической скорости приёма данных, загрузки CPU[5] и состояния очередей. В расчёт включаются только показатели, полученные внутри этой границы; внешние факторы учитываются отдельно только при их явной фиксации в протоколе.

Физическая топология лабораторной сети построена по схеме коммутируемой звезды: каждый узел подключён отдельным соединением к управляемому L_2-коммутатору 1GbE[6]. В эксперименте один передающий узел формирует четыре параллельных UDP-направления к принимающим узлам. Такое описание задаёт условия измерения: физическая схема остаётся неизменной во всех режимах, а профиль передаваемых потоков используется для оценки потерь, задержки, фактической скорости приёма данных, загрузки узла и состояния очередей.

Рис. 1. Граница лабораторной сети и направления UDP-потоков

Рисунок 1 показывает, как построена лабораторная сеть: узлы подключены к L2-коммутатору, а UDP-потоки идут от передающего узла к принимающим узлам. По этой схеме далее определяется, откуда берутся измерения: потери пакетов и фактическая скорость приёма данных фиксируются на стороне получателей, задержка измеряется между узлами, загрузка CPU — на передающем узле, а состояние очередей — на сетевом интерфейсе. Таблица 1 уточняет роль каждого элемента схемы и показывает, какие из них входят в расчёт.

---

[2] (UDP (User Datagram Protocol — протокол пользовательских датаграмм) — транспортный сетевой протокол, передающий данные отдельными датаграммами без предварительного установления соединения. В данной работе по UDP-потокам оцениваются потери, фактическая скорость приёма и влияние сетевых очередей.

[3] L2 (Layer 2 — второй, или канальный, уровень сетевого взаимодействия) — уровень, на котором коммутатор передаёт кадры внутри локальной сети по адресам сетевых интерфейсов.

[4] VLAN (Virtual Local Area Network — виртуальная локальная сеть) — способ логического разделения одной физической сети на независимые сегменты. VLAN-сегмент позволяет отделить, например, прикладной трафик от служебного трафика мониторинга и управления.

[5] CPU (Central Processing Unit — центральный процессор) — основной вычислительный узел компьютера, выполняющий программные инструкции. Загрузка CPU показывает, какая доля вычислительных ресурсов занята в ходе сетевого обмена.

[6] 1GbE (Gigabit Ethernet — гигабитный Ethernet) — стандарт проводной локальной сети с номинальной скоростью передачи данных 1 Гбит/с.

Таблица 1

Элементы, граница эксперимента и статус в расчёте

ЭЛЕМЕНТ НА РИСУНКЕ	ОБОЗНАЧЕНИЕ	РОЛЬ В ЭКСПЕРИМЕНТЕ	ЧТО ИСПОЛЬЗУЕТСЯ В РАСЧЁТЕ
Передающий узел	N_1	Формирует четыре UDP-потока к принимающим узлам.	Загрузка CPU, состояние исходящих очередей, параметры сетевого интерфейса.
Принимающие узлы	N_2–N_5	Принимают UDP-потоки от N1. В данной серии выполняют одинаковую функцию получателей.	Потери UDP-пакетов и фактическая скорость приёма данных на стороне получателей.
Управляемый коммутатор	SW_1	Соединяет узлы по схеме коммутируемой звезды.	Фиксируется как неизменная часть топологии; отдельно не сравнивается между режимами.
Прикладной сегмент	$VLAN_{10}$	Используется для передачи основного UDP-трафика.	По этому сегменту оцениваются потери, задержка и фактическая скорость приёма данных.
Служебный сегмент	$VLAN_{99}$	Используется для мониторинга и управляющего обмена.	Учитывается как возможный источник дополнительной служебной нагрузки.

Файлы $iperf_3$[7], результаты ping/fping[8] и системные показатели CPU/очередей не являются отдельными элементами схемы; они используются как источники числовых данных для расчёта показателей, указанных в таблице.

Обозначения и набор метрик

Перед расчётами фиксируются параметры, которые используются при измерении и обработке результатов. Часть из них задаётся до начала эксперимента: число UDP-направлений, интенсивность нагрузки и длительность прогона. Другая часть получается из журналов измерений: потери пакетов, скорость приёма данных, задержка, загрузка CPU и состояние очередей. Это позволяет отдельно описать условия проведения опыта и показатели, по которым затем сравниваются режимы сети.

Параметры k, b, A, T_{run}, T_{stab} и T_{eff} задают условия проведения эксперимента и остаются одинаковыми для всех сравниваемых режимов. Показатели L_r, G_r, RTT_r, C_r, Q_r и D_r получают по результатам каждого прогона и используют для оценки состояния сети. Интегральный критерий Φ_r рассчитывается после измерений и нужен для сводного сравнения режимов.

В работе контролируются пять основных показателей: потери UDP L_r, фактическая скорость приёма данных G_r, задержка RTT_r, загрузка CPU C_r и состояние очередей Q_r. Интегральный критерий Φ_r строится по четырём первым показателям; состояние очередей Q_r (включая интерфейсные отбросы D_r, drops, overlimits и параметры NIC[9]) используется как диагностический признак и служит для объяснения причины деградации и не входит в Φ_r.

Протоколы измерений

Нагрузка создавалась утилитой $iperf_3$ в UDP-режиме, поскольку она позволяет задать интенсивность потока, длительность прогона и получить отчёт принимающей стороны в машинно-читаемом формате [3, 4, 5]. На узлах N_2—N_5 запускались принимающие процессы $iperf_3$, а узел N_1 одновременно формировал k = 4 UDP-направления с интенсивностью b = 15 Мбит/с на каждое направление. Суммарная заданная нагрузка составляла A = 60 Мбит/с. Размер UDP-датаграммы был принят равным 1400 байт, чтобы оставить запас относительно стандартного Ethernet MTU[10] и снизить риск фрагментации пакетов. Один прогон длился T_{run} = 180 с; первые T_{stab} = 30 с исключались как участок установления потоков, очередей и начальных счётчиков. Основной расчёт выполнялся на интервале T_{eff} = 150 с.

Результаты оценивались по пяти основным показателям: потерям UDP-пакетов L_r, фактической скорости приёма данных на стороне получателей G_r, задержке RTT_r, загрузке CPU передающего узла C_r и состоянию сетевых очередей Q_r. В показатель Q_r включались признаки накопления очереди, backlog, drops, а также интерфейсные отбросы и ошибки D_r, поскольку все эти данные описывают один и тот же участок сетевой

[7] iperf3 — консольная утилита для создания сетевой нагрузки и измерения характеристик передачи данных, включая фактическую скорость, потери и длительность сетевого прогона.

[8] ping и fping — утилиты для проверки доступности сетевых узлов и измерения времени отклика. fping обычно используется для пакетной или массовой проверки нескольких адресов.

[9] NIC (Network Interface Card — сетевая интерфейсная карта, сетевой адаптер) — аппаратный или виртуальный сетевой интерфейс, через который узел подключается к сети.

[10] MTU (Maximum Transmission Unit — максимальный размер передаваемого блока) — наибольший размер сетевого пакета или кадра, который может быть передан без фрагментации. В Ethernet значение MTU учитывается при выборе размера UDP-датаграммы.

Таблица 2

Основные параметры измерения и расчёта

ОБОЗНАЧЕНИЕ	СМЫСЛ	ПОЯСНЕНИЕ
$k = 4$	Число UDP-направлений	В эксперименте один передающий узел отправляет потоки четырём получателям: N_2, N_3, N_4 и N_5.
$b = 15$ Мбит/с	Интенсивность одного UDP-потока	Значение выбрано как одинаковая нагрузка на каждое направление. Это позволяет сравнивать получателей в равных условиях.
$A = 60$ Мбит/с	Суммарная заданная UDP-нагрузка	Рассчитывается как $A = k*b = 4*15 = 60$ Мбит/с.
$T_{run} = 180$ с	Полная длительность одного прогона	Интервал выбран так, чтобы поток успел выйти на устойчивый режим и были получены данные не только по краткому запуску, но и по основной части работы.
$T_{stab} = 30$ с	Начальный участок стабилизации	Первые 30 с не включаются в итоговый расчёт, потому что в начале прогона формируются потоки, очереди и начальные значения счётчиков.
$T_{eff} = 150$ с	Основной интервал расчёта	Рассчитывается как $T_{eff} = T_{run} - T_{stab} = 180 - 30 = 150$ с.
L_r	Потери UDP-пакетов в режиме r, %	Рассчитываются по данным принимающей стороны как доля потерянных пакетов от общего числа отправленных/учтённых пакетов.
G_r	Фактическая скорость приёма данных, Мбит/с	Показывает, какой объём данных реально принят получателями за расчётный интервал.
RTT_r*	Средняя задержка ICMP**, мс	Используется как показатель задержки между узлами в основной части прогона.
C_r	Средняя загрузка CPU передающего узла, %	Показывает, насколько сетевой обмен нагружает узел-источник.
Q_r	Состояние сетевых очередей	Используется для проверки, связана ли деградация с накоплением очередей и отбросами пакетов.
D_r	Интерфейсные отбросы и ошибки	Фиксируются по счётчикам сетевого интерфейса до и после прогона.
$Ф_r$	Интегральный критерий качества режима	Объединяет основные показатели в одну оценку. Чем меньше $Ф_r$, тем лучше режим.
$q = 5$	Число повторов каждого режима	Используется как минимальная серия повторных измерений для расчёта разброса и доверительного интервала. При расширении эксперимента число повторов может быть увеличено.

* RTT (Round Trip Time — время прохождения туда и обратно) — время между отправкой контрольного пакета и получением ответа от удалённого узла. В работе RTT используется как показатель задержки между узлами.

** ICMP (Internet Control Message Protocol — протокол управляющих сообщений Интернета) — служебный сетевой протокол, используемый, в частности, для проверки доступности узлов и измерения времени отклика с помощью ping/fping.

обработки — прохождение пакетов через интерфейс и очередь передачи. Приоритет отдавался данным принимающей стороны iperf$_3$, так как именно получатель фиксирует доставленный объём данных и фактические потери.

Показатель Q_r рассматривается как расширенная характеристика состояния сетевой обработки. Поэтому в него включаются не только значения очередей qdisc[11], но и связанные с ними признаки: интерфейсные

[11] qdisc (queueing discipline — дисциплина очереди) — механизм управления очередью пакетов на сетевом интерфейсе. Через

Таблица 3

Источники данных для пяти основных показателей

ОСНОВНОЙ ПОКАЗАТЕЛЬ	ИСТОЧНИК ДАННЫХ	ПЕРИОД ФИКСАЦИИ	ЗАЧЕМ ИЗМЕРЯЕТСЯ
Потери UDP-пакетов L_r	JSON*-отчёт $iperf_3$ на стороне получателя	Каждый прогон, интервал T_{eff}	Показывает, какая доля пакетов не была доставлена до принимающих узлов.
Фактическая скорость приёма данных G_r	receiver-side JSON $iperf_3$: bits_per_second, bytes, seconds**	Каждый прогон, интервал T_{eff}	Показывает объём данных, реально принятый получателями за расчётный интервал.
Задержка RTT_r	ping/fping	Основной интервал после стабилизации	Используется для оценки времени отклика между узлами после выхода потока на рабочий режим.
Загрузка CPU передающего узла C_r	mpstat, pidstat, top***	Во время основного интервала измерения	Показывает, насколько передающий узел загружен при формировании UDP-потоков.
Состояние сетевых очередей Q_r	tc -s qdisc; ip -s link; ethtool -S; ethtool -c/-k/-a****	До, во время и после прогона; параметры NIC — перед серией и после коррекции	Используется для проверки накопления очередей, drops, overlimits, интерфейсных отбросов, ошибок и параметров NIC.

* JSON (JavaScript Object Notation — текстовый формат обмена структурированными данными) — формат представления данных в виде пар «ключ — значение». В работе JSON используется как машинно-читаемый формат отчёта iperf3.

** bits_per_second, bytes, seconds — имена полей JSON-отчёта iperf3, обозначающие соответственно скорость в битах в секунду, объём переданных или принятых данных в байтах и длительность измеренного интервала.

*** mpstat, pidstat и top — системные утилиты мониторинга, применяемые для оценки загрузки процессора и активности процессов во время сетевого эксперимента.

**** tc, ip и ethtool — системные утилиты для просмотра и настройки сетевых параметров узла. В данной работе они используются для анализа очередей, интерфейсных счётчиков и параметров сетевого адаптера.

отбросы D_r, ошибки, drops, overlimits[12], а также параметры сетевого адаптера. [6,7,8] Такое объединение позволяет сохранить пять основных показателей оценки и одновременно не терять технические признаки, которые помогают объяснить причину деградации.

Режимы модели и адресная коррекция сетевой обработки

В эксперименте сравниваются три состояния одной и той же лабораторной сети. Они соответствуют этапам спиральной модели: сначала фиксируется исходное состояние R_0, затем расширяется наблюдаемость R_1, после этого выполняется адресная коррекция сетевой обработки R_2. Под адресной коррекцией понимается не произвольная настройка сети, а изменение того участка сетевой обработки, который связан с ухудшением пяти контролируемых показателей: потерь пакетов, фактической скорости приёма данных, задержки, загрузки передающего узла и состояния очередей. Поэтому корректирующие действия выбираются после расширения наблюдаемости и направляются не на всю сеть сразу, а на выявленный участок деградации. В данной серии такими действиями являются сглаживание очередей, выравнивание подачи потоков, снижение служебной конкуренции, приоритет прикладного трафика и проверка обработки сетевых прерываний.

Такое разделение необходимо для корректного сравнения режимов. Если одновременно менять оборудование, топологию, нагрузку и настройки, то невозможно определить, за счёт чего улучшился результат. Поэтому в работе сравниваются режимы, в которых условия сетевого обмена сохраняются, а изменения вносятся поэтапно и проверяются по одним и тем же показателям.

qdisc можно оценивать накопление очереди, ограничения и отбрасывание пакетов.

[12] backlog, drops и overlimits — диагностические признаки состояния сетевой очереди: backlog показывает накопление пакетов в очереди, drops — число отброшенных пакетов, overlimits — события превышения заданных ограничений обработки очереди.

Таблица 4

Режимы эксперимента и логика корректирующих действий

РЕЖИМ	РОЛЬ В СПИРАЛЬНОЙ МОДЕЛИ	ЧТО ДОБАВЛЯЕТСЯ ИЛИ ИЗМЕНЯЕТСЯ	ЧТО ПРОВЕРЯЕТСЯ
R_0	Исходное состояние сети	Корректирующие действия не применяются. Фиксируются базовые значения потерь, скорости приёма данных, задержки, загрузки CPU и состояния очередей.	Получение базы для сравнения последующих режимов.
R_1	Расширение наблюдаемости	Добавляются дополнительные признаки сетевой обработки: состояние очередей, drops, backlog, интерфейсные счётчики, загрузка CPU, данные принимающей стороны и параметры сетевого адаптера.	Определяется, с чем связана деградация: с очередями, нагрузкой передающего узла.
R_2	Адресная коррекция после диагностики	Применяются действия, направленные на выявленный участок деградации: сглаживание очередей, выравнивание подачи потоков, снижение служебной конкуренции VLAN99, приоритет VLAN10, проверка режима обработки сетевых прерываний.	Проверяется, улучшается ли группа показателей после коррекции: потери, скорость приёма данных, задержка, загрузка CPU и состояние очередей.

Проверка Net DIM[13] относится к режиму R_2, потому что она связана не с расширением наблюдаемости, а с качеством обработки сетевых прерываний на сетевом адаптере. В этой работе Net DIM рассматривается как один из возможных механизмов адресной коррекции: если адаптивная модерация прерываний поддерживается драйвером, она может снижать лишнюю нагрузку на CPU и уменьшать влияние сетевой обработки на очереди. Если такая поддержка отсутствует, в протоколе фиксируется, что этот механизм не применялся, а режим R_2 оценивается по остальным корректирующим действиям.

Формальная модель оценки и статистическая проверка

Расчёт начинается не с итоговых средних значений, а с первичных данных каждого прогона. Для режима r и повтора s фиксируются значения потерь пакетов, скорости приёма данных, задержки, загрузки CPU и состояния очередей. Источниками являются отчёты принимающей стороны $iperf_3$, результаты ICMP-измерений, системные показатели передающего узла и счётчики сетевого интерфейса. Поэтому каждая итоговая величина сначала получается из журнала измерений, а затем используется в статистической обработке.

Для каждого показателя формируется вектор повторов:

$X_r = \{X_{r,1}; X_{r,2}; \ldots; X_{r,q}\}$, где:

q — число повторов режима.

В этой записи X может обозначать любой из рассчитываемых показателей L, G, RTT, C или Q.

Среднее значение показателя в режиме r рассчитывается по формуле:

$$M_r = \frac{1}{q}\sum_{s=1}^{q} X_{r,s}$$

Выборочное стандартное отклонение показывает разброс значений между повторами:

$$SD_r = \sqrt{\frac{\sum_{s=1}^{q}(X_{r,s} - M_r)^2}{q-1}}$$

Стандартная ошибка среднего рассчитывается как:

$$SE_r = \frac{SD_r}{\sqrt{q}}$$

Для оценки среднего значения в каждом режиме в работе принимается уровень значимости $\alpha = 0{,}05$. Ему соответствует доверительная вероятность $1 - \alpha = 0{,}95$, то есть 95% доверительный интервал. Поскольку число повторов невелико, доверительный интервал строится не по нормальному распределению, а по распределению Стьюдента [9, 10].

Для двустороннего 95% доверительного интервала используется квантил:

$$t_{1-\frac{\alpha}{2};q-1}$$

Тогда 95% доверительный интервал имеет вид:

$$CI_{95} = M_r \pm t_{0{,}975;q-1} SE_r$$

[13] Net DIM (Network Dynamic Interrupt Moderation — динамическая модерация сетевых прерываний) — механизм адаптивного управления частотой сетевых прерываний от адаптера к процессору. Он может снижать лишнюю нагрузку на CPU, если поддерживается драйвером и сетевым адаптером.

При $q = 5$ число степеней свободы равно:

$$df = q - 1$$

DP-пакеты рассчитываются по данным принимающей стороны iperf$_3$:

$$L_{r,s} = \frac{LostPackets_{r,s}}{Packets_{r,s}} 100\%$$

Фактическая скорость приёма данных в повторе s для режима r определяется по принимающей стороне iperf$_3$:

$$G_{r,s} = \frac{8bytes_{r,s}}{T_{eff}}, 0 \le G_{r,s} \le A,$$ где:

8 — количество бит в 1 байте.

Средняя задержка ICMP в повторе s вычисляется по результатам ping/fping как среднее значение по выборке задержек:

$$RTT_{r,s} = \frac{1}{n_{r,s}} \sum_{i=1}^{n_{r,s}} RTT_{r,s}^{(i)}$$

Средняя загрузка CPU передающего узла определяется по данным системных утилит (mpstat, pidstat, top):

$$C_{r,s} = \frac{1}{m_{r,s}} \sum_{j=1}^{m_{r,s}} CPU_{r,s}^{(j)}$$

Показатель состояния сетевых очередей агрегирует признаки qdisc/backlog/drops за прогон:

$$Q_{r,s} = f_Q(qdisc_{r,s}, backlog_{r,s}, drops_{r,s})$$

Интерфейсные отбросы и ошибки учитываются отдельным показателем:

$$D_{r,s} = f_D(err_{r,s}, drop_{r,s}, overlim_{r,s})$$

Интегральный критерий качества режима строится на средних значениях основных метрик:

$$\Phi_r = \frac{1}{4}\left(\frac{L_r}{L_0} + \frac{RTT_r}{RTT_0} + \frac{C_r}{C_0} + \frac{G_0}{G_r}\right)$$

Чем меньше Фr, тем лучше режим: снижение потерь, уменьшение задержки и загрузки CPU, а также рост фактической скорости приёма данных приводят к уменьшению всех слагаемых и, следовательно, к снижению Φ_r.

Первичные данные и результаты

На графике показаны результаты нескольких независимых прогонов для каждого режима. Эти точки и столбцы отражают непосредственно измеренные значения и служат основой для расчёта описательных статистик и 95 % доверительных интервалов. В данной серии использовано пять прогонов на режим, однако описанный способ построения графика и обработки данных сохраняется при любом числе прогонов, достаточном для статистической оценки.

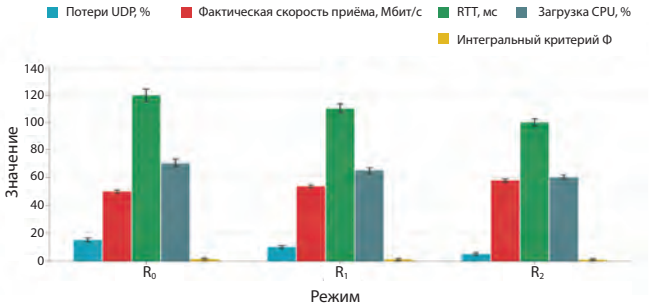

Рис. 2. Показатели сети по режимам R_0-R_2

Для каждого показателя и режима рассчитывались среднее значение, выборочное стандартное отклонение, стандартная ошибка среднего и двусторонний 95 % доверительный интервал. Эти характеристики позволяют оценить не только направление изменения метрик между режимами, но и разброс результатов по повторам, а также убедиться, что наблюдаемый эффект выходит за пределы случайных колебаний.

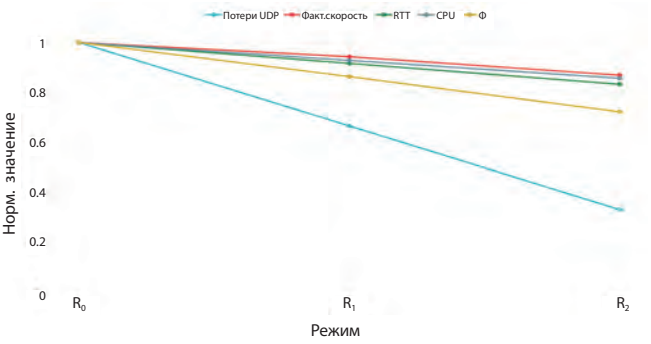

Рис. 3. Нормированные показатели по режимам

Сравнение трёх режимов показывает, что сам этап расширения наблюдаемости R_1 выполнял прежде всего диагностическую функцию. В режиме R_1 к исходным измерениям были добавлены признаки сетевой обработки: состояние очередей, backlog, drops, интерфейсные счётчики, загрузка CPU и параметры сетевого адаптера. Эти данные позволили связать ухудшение показателей не с изменением физической топологии или величины заданной нагрузки, а с локальным участком сетевой обработки в узле-источнике.

При этом R_1 не являлся конечным улучшенным режимом: по средним значениям показатели оставались хуже, чем после адресной коррекции R_2. Потери UDP составили около 10,0% в R_1 против 5,0% в R_2, фактическая скорость приёма данных — 54,0 против 57,5 Мбит/с, средняя задержка RTT — 110 против 100 мс, загрузка CPU передающего узла — 65 против 60%. Интегральный критерий качества режима снизился с 1,000 в R0 до 0,860 в R_1 и до 0,723 в R_2.

Следовательно, вывод о недостаточности одной только наблюдаемости основан на сопоставлении промежуточного режима R_1 с итоговым режимом R_2. Расширение наблюдаемости позволило выявить источник деградации и выбрать корректирующее действие, однако согласованное улучшение всех основных метрик было достигнуто только после адресной коррекции сетевой обработки.

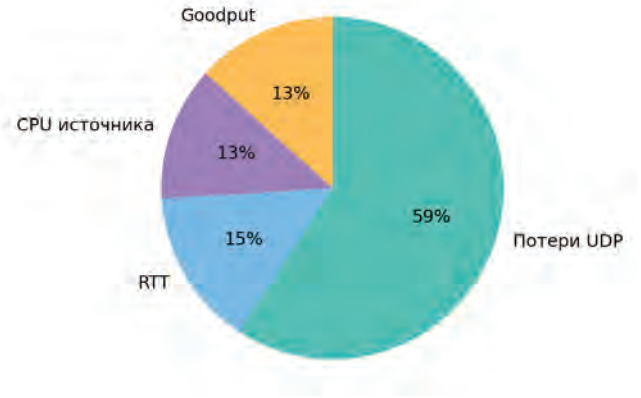

Рис. 4. Вклад показателей критерия Ф при переходе от R_0 к R_2; показатель Goodput[14] соответствует фактической полезной скорости приёма данных

Обсуждение

Во всех режимах эксперимента физическая топология и нагрузка на стенд оставались неизменными: схема соединений не менялась, а предложенная нагрузка сохранялась на уровне A = 60 Мбит/с. Поэтому наблюдаемое улучшение показателей нельзя объяснить ни увеличением пропускной способности канала, ни снижением внешней нагрузки. Оно связано с локальной коррекцией сетевой обработки в узле-источнике (настройкой очередей и алгоритмов обработки трафика), которая привела к уменьшению потерь и задержек без изменения топологии, и нагрузки.

Корректный вывод состоит в том, что коррекция в одной точке улучшила суммарные показатели нескольких исходящих направлений. В представленной серии измерений делается вывод только о влиянии локальной коррекции в узле-источнике на совокупные показатели исходящих направлений. Вопрос о возможном каскадном распространении эффекта по последовательной цепочке узлов в данной работе не анализируется, поскольку такая конфигурация сети не задавалась и характеристики промежуточных узлов отдельно не измерялись.

Заключение

В статье предложена методика статистической оценки локальной сетевой деградации в лабораторной сети, используемой для проверки контуров информационной безопасности. Методика основана на последовательной схеме: задание границы эксперимента, фиксация исходного состояния, расширение наблюдаемости, выявление участка деградации, адресная коррекция сетевой обработки и повторное измерение результата. Для сопоставления режимов использованы пять основных показателей: потери пакетов, фактическая скорость приёма данных на стороне получателей, задержка, загрузка передающего узла и состояние очередей.

Полученные результаты показали, что расширение наблюдаемости является необходимым, но не достаточным этапом. Улучшение достигается тогда, когда дополнительные измерения используются для выбора конкретного корректирующего действия. В итоговом режиме снижение потерь, уменьшение задержки, рост фактической скорости приёма данных и снижение загрузки передающего узла подтвердили согласованное улучшение сетевых показателей без изменения физической топологии и без уменьшения заданной нагрузки.

Практическая значимость работы состоит в том, что предложенный порядок позволяет обосновывать сетевую коррекцию до замены оборудования или перестройки схемы соединений [11, 12]. Методика может применяться для анализа лабораторных и пилотных сетевых участков, где требуется не только зафиксировать ухудшение, но и показать, за счёт какого изменения достигается улучшение. Полученный вывод относится к рассматриваемой конфигурации с одним передающим узлом и несколькими принимающими направлениями; исследование последовательного каскадного распространения эффекта требует отдельной экспериментальной постановки [13—15]. Дальнейшее развитие методики может быть связано с динамическим контролем функционирования защищаемых автоматизированных систем и применением методов математической статистики для выявления сетевых вторжений и аномалий трафика [16, 17].

[14] Goodput — полезная скорость доставки данных, то есть скорость передачи полезной нагрузки, реально полученной принимающей стороной без учёта служебных накладных расходов и потерь.

Литература

1. Alkenani J. Network Monitoring Measurements for Quality of Service: A Review / J. Alkenani, K.A. Nassar // Iraqi Journal for Electrical and Electronic Engineering. 2022. Vol. 18, № 2. P. 33—42. DOI: 10.37917/ijeee.18.2.5
2. Graf F. Monitoring Performance Metrics in Low Power Wireless Systems / F. Graf, T. Watteyne, M. Villnow // ICT Express. 2024. Vol. 10, № 5. P. 989—1018. DOI: 10.1016/j.icte.2024.08.004
3. Polverini M. Reducing the In Band Network Telemetry Overhead through the Spatial Sampling: Theory and Experimental Results / M. Polverini [et al.] // Computer Networks. 2024. Vol. 242. Article 110269. DOI: 10.1016/j.comnet.2024.110269
4. Zeng X. INT MC: Low Overhead In Band Network Wide Telemetry Based on Matrix Completion / X. Zeng [et al.] // Proceedings of the ACM on Measurement and Analysis of Computing Systems. 2024. Vol. 8, № 3. P. 1—30. DOI: 10.1145/3700433
5. Xu Z. Information Sensitive In Band Network Telemetry in P4 Based Programmable Data Plane / Z. Xu, Z. Lu, Z. Zhu // IEEE/ACM Transactions on Networking. 2024. Vol. 32. P. 5081—5096. DOI: 10.1109/TNET.2024.3448244
6. Alshahrani A. A Fully Adaptive Active Queue Management Method for Congestion Prevention at the Router Buffer / A. Alshahrani [et al.] // Computers, Materials and Continua. 2023. Vol. 77, № 2. P. 1679—1698. DOI: 10.32604/cmc.2023.043545
7. Abdel Jaber H. Performance Analysis of Diverse Active Queue Management Algorithms / H. Abdel Jaber // International Journal of Networked and Distributed Computing. 2025. Vol. 13. Article 15. DOI: 10.1007/s44227-025-00056-1
8. Singha S. Active Queue Management in RED Considering Critical Point on Target Queue / S. Singha, B. Jana, N.K. Mandal // Journal of Interconnection Networks. 2021. Vol. 21, № 3. Article 2150017. DOI: 10.1142/S0219265921500171
9. Najmi A. How to Choose and Interpret a Statistical Test? An Update for Budding Researchers / A. Najmi, B. Sadasivam, A. Ray // Journal of Family Medicine and Primary Care. 2021. Vol. 10, № 8. P. 2763—2767. DOI: 10.4103/jfmpc.jfmpc_433_21
10. Ponce Renova H.F. Comparing Effect Sizes and Their Confidence Intervals: A Primer on Equivalence Testing in Educational Research / H.F. Ponce Renova // Journal of New Approaches in Educational Research. 2022. Vol. 11, № 2. P. 209—225. DOI: 10.7821/naer.2022.7.930
11. Manzanares Lopez P. Passive In Band Network Telemetry Systems: The Potential of Programmable Data Plane on Network Wide Telemetry / P. Manzanares Lopez, J.P. Muñoz Gea, J. Malgosa Sanahuja // IEEE Access. 2021. Vol. 9. P. 20391—20409. DOI: 10.1109/ACCESS.2021.3055462
12. Yaseen N. From Counters to Telemetry: A Survey of Programmable Network Wide Monitoring / N. Yaseen // Network. 2025. Vol. 5, № 3. Article 38. DOI: 10.3390/network5030038
13. Tan L. In Band Network Telemetry: A Survey / L. Tan [et al.] // Computer Networks. 2021. Vol. 186. Article 107763. DOI: 10.1016/j.comnet.2020.107763
14. Yang Z. A Systematic Literature Review of Methods and Datasets for Anomaly Based Network Intrusion Detection / Z. Yang [et al.] // Computers & Security. 2022. Vol. 116. Article 102675. DOI: 10.1016/j.cose.2022.102675
15. Schummer P. Machine Learning Based Network Anomaly Detection: Design, Implementation, and Evaluation / P. Schummer [et al.] // AI. 2024. Vol. 5, № 4. P. 2967—2983. DOI: 10.3390/ai5040143
16. Котенко И.В. Динамическая модель контроля функционирования для предупреждения компьютерных атак / И.В. Котенко, И.Б. Саенко, Р.И. Захарченко, Д.В. Величко // Правовая информатика. 2024. № 2. С. 35—43. DOI: 10.21681/1994-1404-2024-2-35-43.
17. Котенко И.В. Методика обнаружения сетевых вторжений на основе интеграции методов вейвлет-анализа и математической статистики / И.В. Котенко, И.Б. Саенко, П.В. Бортникер // Правовая информатика. 2024. № 4. С. 23—31. DOI: 10.24412/1994-1404-2024-4-23-31.

STATISTICAL ASSESSMENT OF THE LOCAL CORRECTION OF NETWORK DEGRADATION IN THE LABORATORY INFORMATION SECURITY NETWORK

Isaev N.A.[15]

Keywords: *network observability, network metrics, confidence intervals, Student's t-test, UDP streams, integral quality criterion of the mode, targeted correction, physical network topology.*

Abstract

Purpose of work. *To develop and verify an approach that makes it possible to assess how a local change in network processing affects the overall state of a laboratory network used in information security tasks. The main task is to link the deterioration of network indicators with a measurable cause and to verify the correction result not based on a single indicator, but based on a group of interrelated metrics.*

Research methods. *The work was carried out on a controlled network configuration consisting of a transmitting node, four receiving nodes, a managed link-layer switch, and two logical traffic segments. The load was generated by parallel unidirectional streams of the User Datagram Protocol (UDP), and measurements were taken at the receivers' side and the transmitting node. The initial state of the network, the state after expanding observability, and the state after targeted correction were compared. For data processing, repeated runs, mean values, confidence intervals, and Student's t-test for related samples were applied.*

Results of the study. *The comparison of R0, R1 and R2 showed that expanding observability plays a diagnostic rather than corrective role. It made it possible to identify the local degradation section using queue, interface and CPU indicators, but the best network state was achieved only after targeted correction. Compared with R1, R2 reduced UDP packet loss from about 10.0 to 5.0%, increased the actual receiving rate from 54.0 to 57.5 Mbit/s, decreased RTT from 110 to 100 ms, and reduced the transmitter CPU load from 65 to 60%. Therefore, expanding observability alone should be considered a necessary diagnostic stage, but not a sufficient condition for improving the network state. The greatest effect is achieved after identifying the local source of degradation and correcting the corresponding section of network processing. In the measured series, packet loss and latency decreased, the load on the transmitting node reduced, the actual data reception rate increased, and the queue state stabilized. The integral assessment confirmed a consistent improvement in a group of indicators, rather than in a single metric. This makes it possible to use the proposed approach in the field of information security for experimental diagnostics of network segments where it is necessary to justify corrective action before replacing equipment, changing the topology, or reducing the specified load. In practical terms, the work demonstrates how the transition from observation to verified correction makes network analysis more evidence-based.*

References

1. Alkenani J. Network Monitoring Measurements for Quality of Service: A Review / J. Alkenani, K.A. Nassar // Iraqi Journal for Electrical and Electronic Engineering. 2022. Vol. 18, № 2. P. 33—42. DOI: 10.37917/ijeee.18.2.5
2. Graf F. Monitoring Performance Metrics in Low Power Wireless Systems / F. Graf, T. Watteyne, M. Villnow // ICT Express. 2024. Vol. 10, № 5. P. 989—1018. DOI: 10.1016/j.icte.2024.08.004
3. Polverini M. Reducing the In Band Network Telemetry Overhead through the Spatial Sampling: Theory and Experimental Results / M. Polverini [et al.] // Computer Networks. 2024. Vol. 242. Article 110269. DOI: 10.1016/j.comnet.2024.110269
4. Zeng X. INT MC: Low Overhead In Band Network Wide Telemetry Based on Matrix Completion / X. Zeng [et al.] // Proceedings of the ACM on Measurement and Analysis of Computing Systems. 2024. Vol. 8, № 3. P. 1—30. DOI: 10.1145/3700433
5. Xu Z. Information Sensitive In Band Network Telemetry in P4 Based Programmable Data Plane / Z. Xu, Z. Lu, Z. Zhu // IEEE/ACM Transactions on Networking. 2024. Vol. 32. P. 5081—5096. DOI: 10.1109/TNET.2024.3448244

[15] ***Nikolay A. Isaev***, *Ph.D. student, Moscow Witte University, Moscow, Russia. ORCID: 0009-0007-3987-1670. E-mail: supercopen@yandex.ru*

6. Alshahrani A. A Fully Adaptive Active Queue Management Method for Congestion Prevention at the Router Buffer / A. Alshahrani [et al.] // Computers, Materials and Continua. 2023. Vol. 77, № 2. P. 1679—1698. DOI: 10.32604/cmc.2023.043545
7. Abdel Jaber H. Performance Analysis of Diverse Active Queue Management Algorithms / H. Abdel Jaber // International Journal of Networked and Distributed Computing. 2025. Vol. 13. Article 15. DOI: 10.1007/s44227-025-00056-1
8. Singha S. Active Queue Management in RED Considering Critical Point on Target Queue / S. Singha, B. Jana, N.K. Mandal // Journal of Interconnection Networks. 2021. Vol. 21, № 3. Article 2150017. DOI: 10.1142/S0219265921500171
9. Najmi A. How to Choose and Interpret a Statistical Test? An Update for Budding Researchers / A. Najmi, B. Sadasivam, A. Ray // Journal of Family Medicine and Primary Care. 2021. Vol. 10, № 8. P. 2763—2767. DOI: 10.4103/jfmpc.jfmpc_433_21
10. Ponce Renova H.F. Comparing Effect Sizes and Their Confidence Intervals: A Primer on Equivalence Testing in Educational Research / H.F. Ponce Renova // Journal of New Approaches in Educational Research. 2022. Vol. 11, № 2. P. 209—225. DOI: 10.7821/naer.2022.7.930
11. Manzanares Lopez P. Passive In Band Network Telemetry Systems: The Potential of Programmable Data Plane on Network Wide Telemetry / P. Manzanares Lopez, J.P. Muñoz Gea, J. Malgosa Sanahuja // IEEE Access. 2021. Vol. 9. P. 20391—20409. DOI: 10.1109/ACCESS.2021.3055462
12. Yaseen N. From Counters to Telemetry: A Survey of Programmable Network Wide Monitoring / N. Yaseen // Network. 2025. Vol. 5, № 3. Article 38. DOI: 10.3390/network5030038
13. Tan L. In Band Network Telemetry: A Survey / L. Tan [et al.] // Computer Networks. 2021. Vol. 186. Article 107763. DOI: 10.1016/j.comnet.2020.107763
14. Yang Z. A Systematic Literature Review of Methods and Datasets for Anomaly Based Network Intrusion Detection / Z. Yang [et al.] // Computers & Security. 2022. Vol. 116. Article 102675. DOI: 10.1016/j.cose.2022.102675
15. Schummer P. Machine Learning Based Network Anomaly Detection: Design, Implementation, and Evaluation / P. Schummer [et al.] // AI. 2024. Vol. 5, № 4. P. 2967—2983. DOI: 10.3390/ai5040143
16. Kotenko I.V. Dinamicheskaia model' kontrolia funktsionirovaniia dlia preduprezhdeniia komp'iuternykh atak / I.V. Kotenko, I.B. Saenko, R.I. Zakharchenko, D.V. Velichko // Pravovaia informatika. 2024. No. 2. S. 35—43. DOI: 10.21681/1994-1404-2024-2-35-43.
17. Kotenko I.V. Metodika obnaruzheniia setevykh vtorzhenii na osnove integratsii metodov veivlet-analiza i matematicheskoi statistiki / I.V. Kotenko, I.B. Saenko, P.V. Bortniker // Pravovaia informatika. 2024. No. 4. S. 23—31. DOI: 10.24412/1994-1404-2024-4-23-31.