Ежегодная международная научно-практическая конференция «РусКрипто'2022»

Нахождение пороговых значений сетевой атаки по неполным данным sFlow

Докладчик: Сухов Андрей Михайлович

Терехов Александр Игоревич, НИУ ВШЭ
Сагатов Евгений Собирович, к.т.н., доцент, НИУ ВШЭ
Сухов Андрей Михайлович, д.т.н., профессор, ДКИ МИЭМ, НИУ ВШЭ

Актуальность

Актуальность данного исследования обусловлена быстрым ростом объема трафика, передаваемого по сети, и необходимостью анализа данного трафика.

Новизна

Ранее метод пороговых значений исследовался применительно к анализу всех пакетов, передаваемых по сети.

В настоящей работе:

- Проведено исследование метода пороговых значений для выборочного анализа сетевого трафика.
- Найдена зависимость порогового значения от размера выборки пакетов.
- Полученная зависимость подтверждена экспериментально в ходе эксперимента в реальной сети.

Постановка задач

- Определить теоретическую зависимость порогового значения от величины выборки
- Определить предельное разрешение выборки, при котором данное пороговое значение может быть обнаружено
- Экспериментально подтвердить найденную зависимость порогового значения от величины выборки

Пороговые значения

Закон Зипфа: $p_i = \frac{p_1}{i^\alpha}$

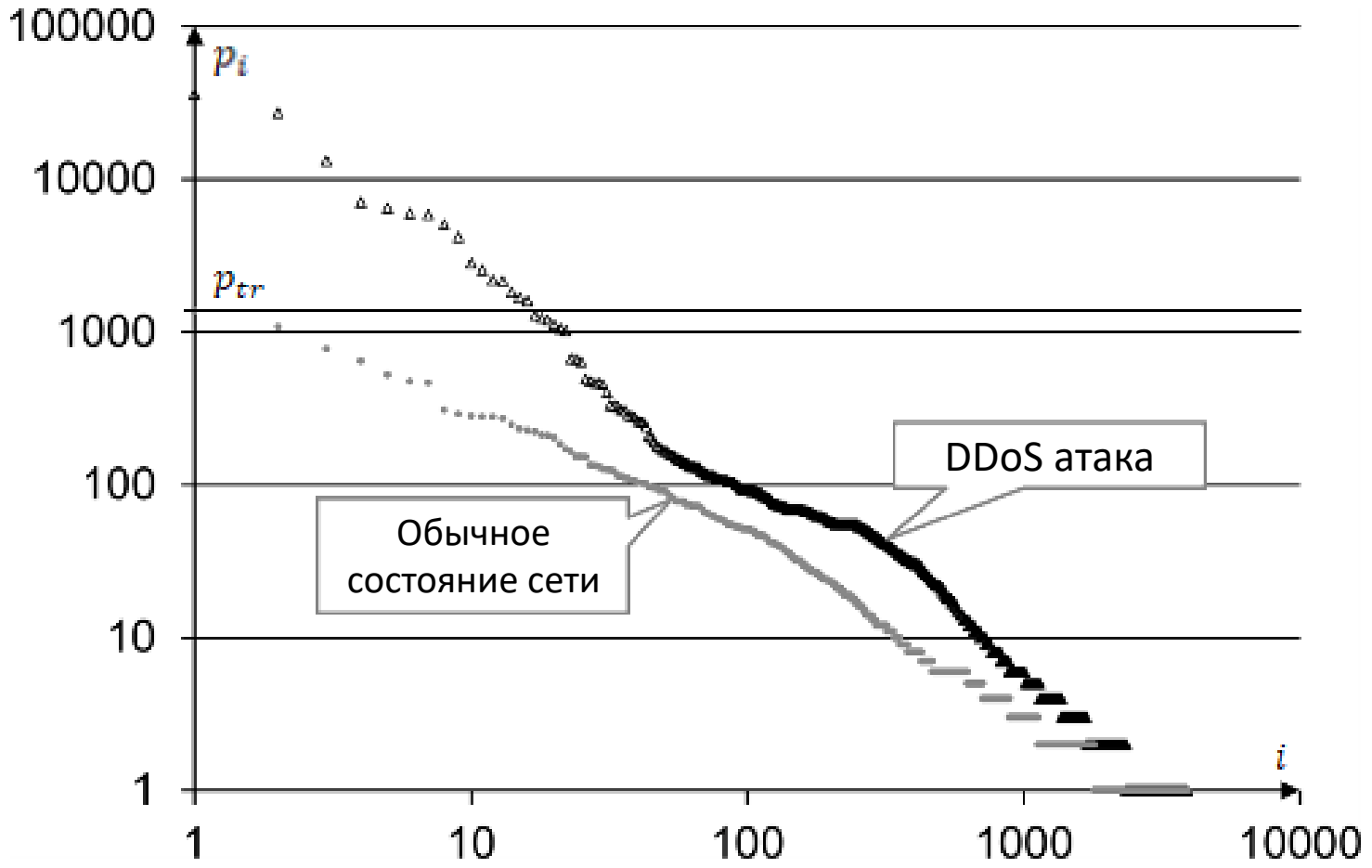
$$\lg p_i = \lg p_1 - \alpha \lg i$$

p_1 – наибольшее значение исследуемой величины

i – ранг

α – показатель степени распределения.

p_{tr} – пороговое значение



Выборочный анализ трафика

$p_{tr} \rightarrow \frac{p_{tr}}{N}$

$\lg p_i = \lg p_1 - \lg N - \alpha \lg i$

$\frac{p_{tr}}{N_{lim}} = 1 \rightarrow$ предел, ниже которого вторжение с порогом p_{tr} не будет обнаружено

N – частота выборки

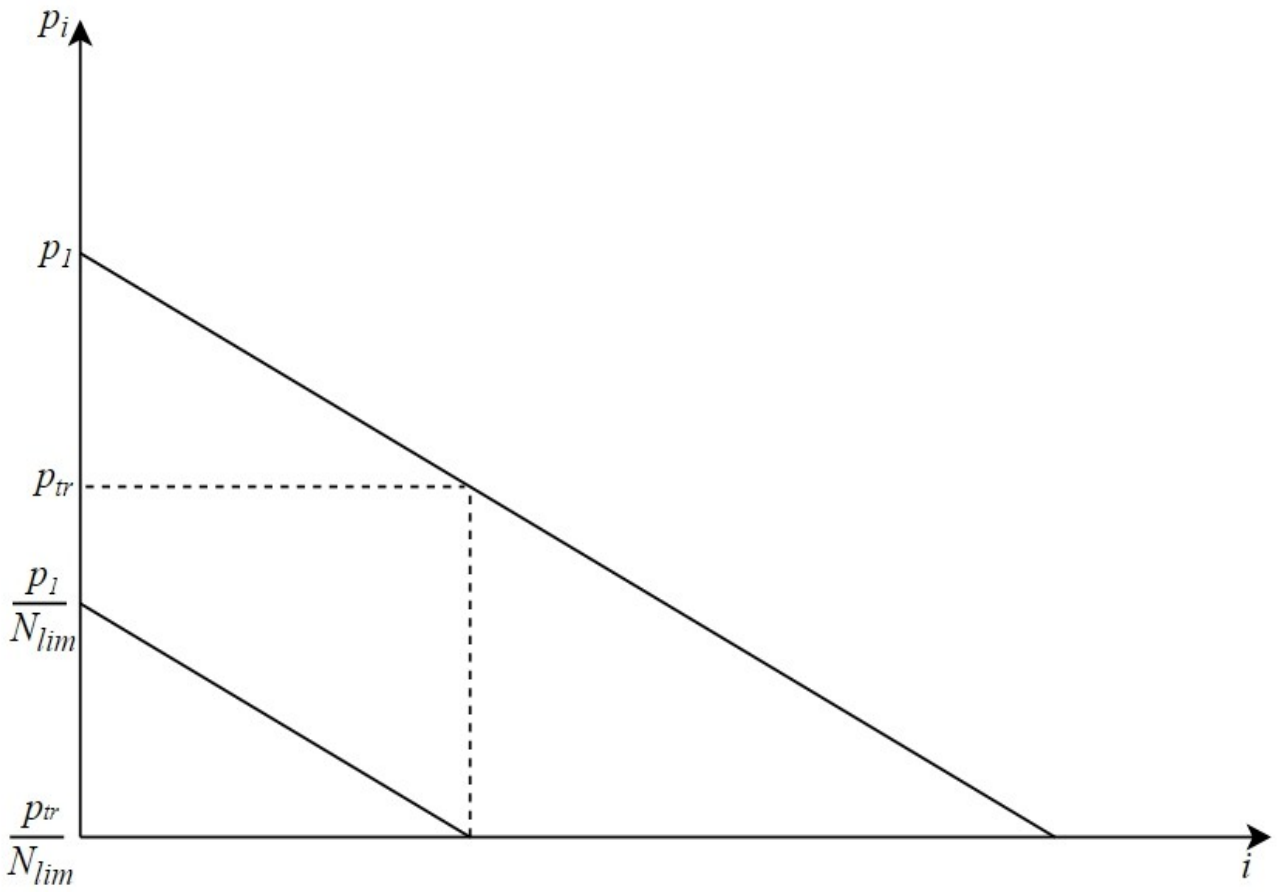
N_{lim} – предельная частота выборки

p_1 – наибольшее значение исследуемой величины

i – ранг

α – показатель степени распределения.

p_{tr} – пороговое значение



Эксперимент по проверке гипотезы

Проверяемая гипотеза: $p_k^{tr} * N_k = \text{const}$

p_k^{tr} – измеряемое в ходе атаки значение сетевой величины

N_k – частота выборки

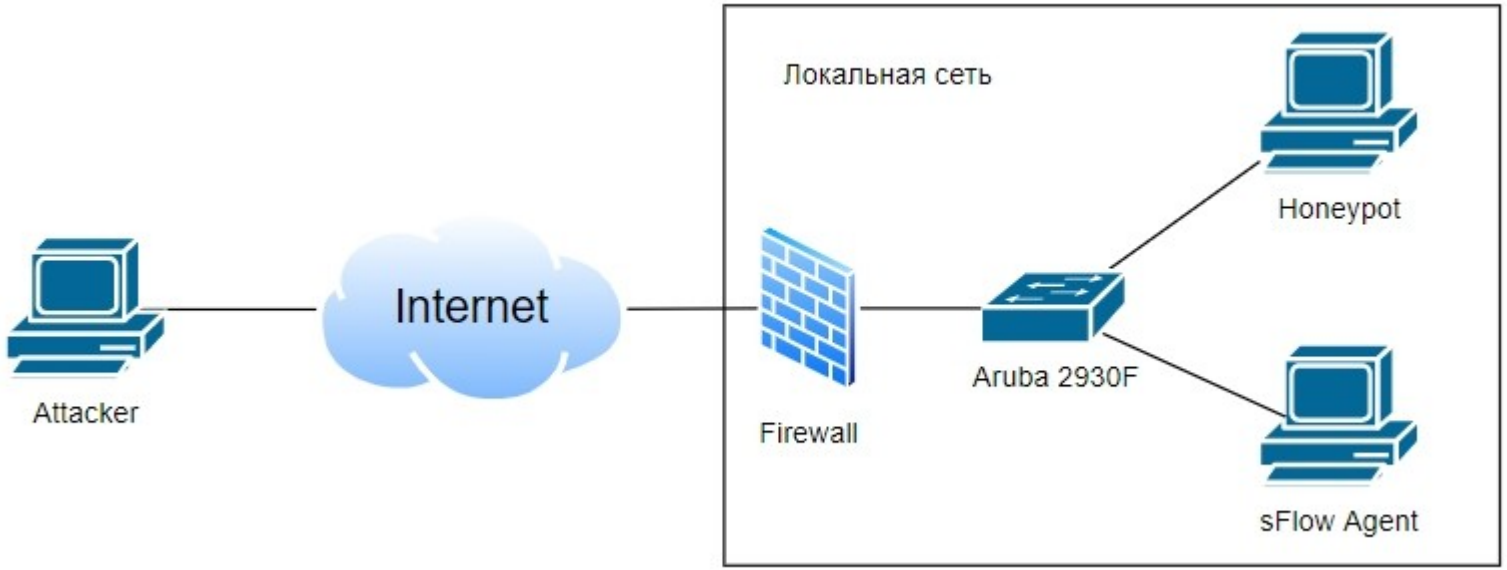
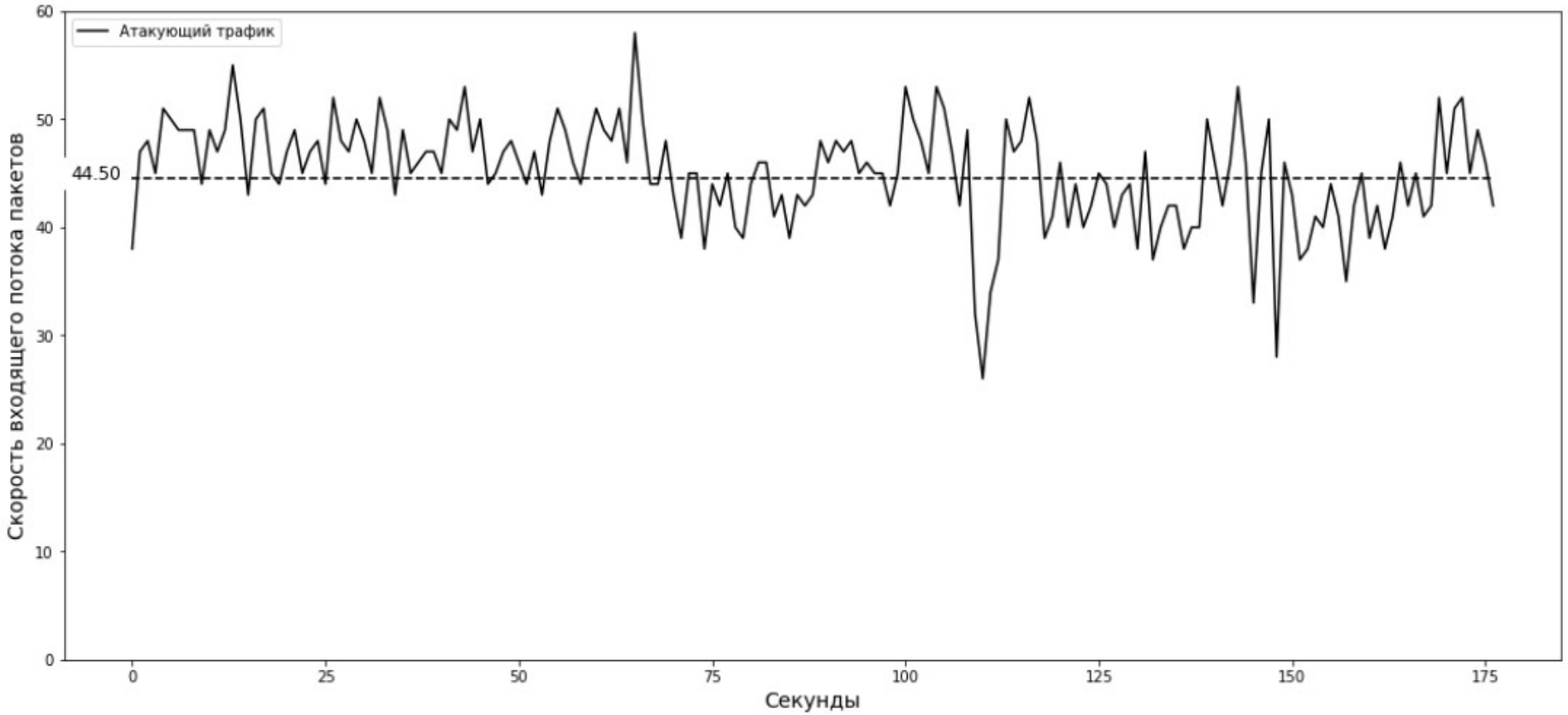


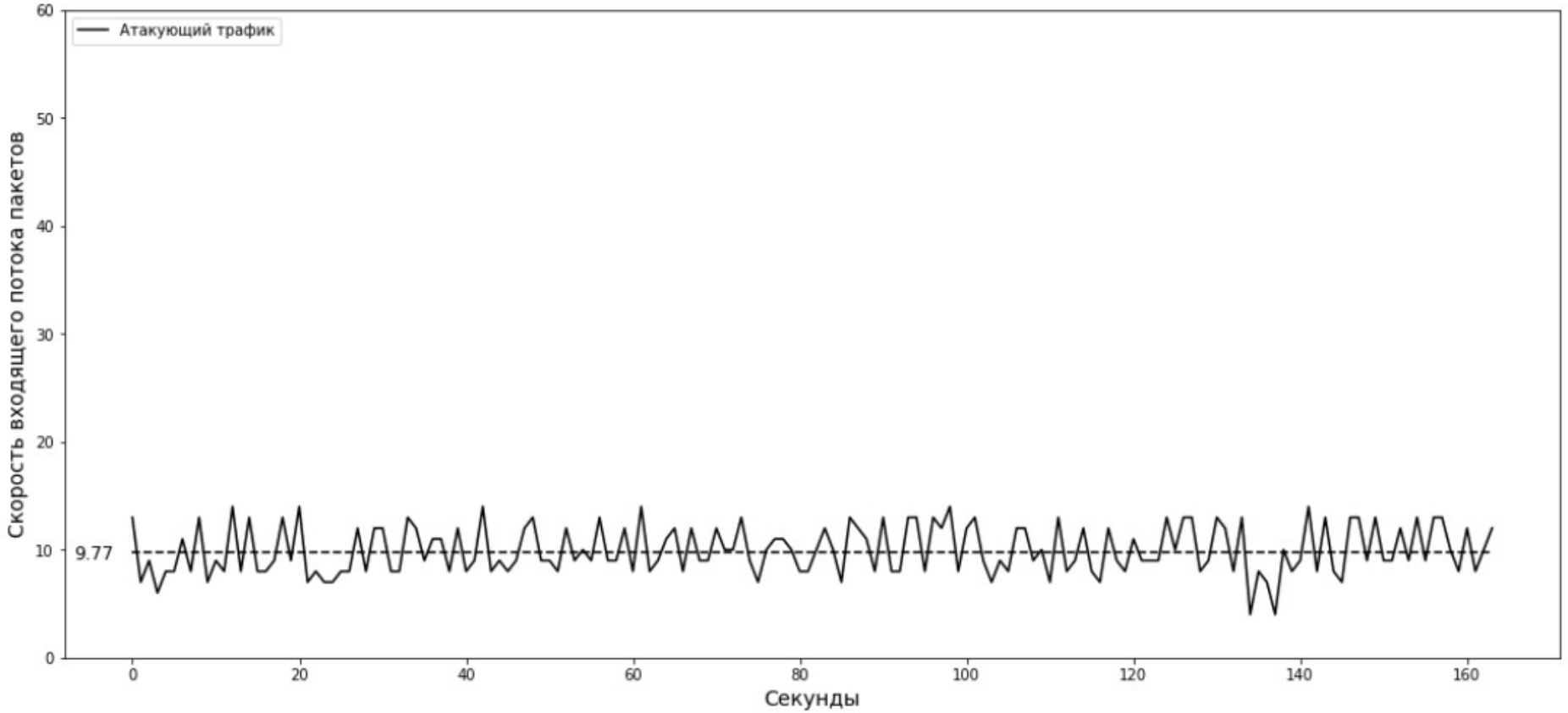
Схема сетевого полигона для проведения экспериментов

Результаты эксперимента



Временная зависимость для скорости входящего потока пакетов $B_N(t)$ при выборке «1 из 50»

Результаты эксперимента



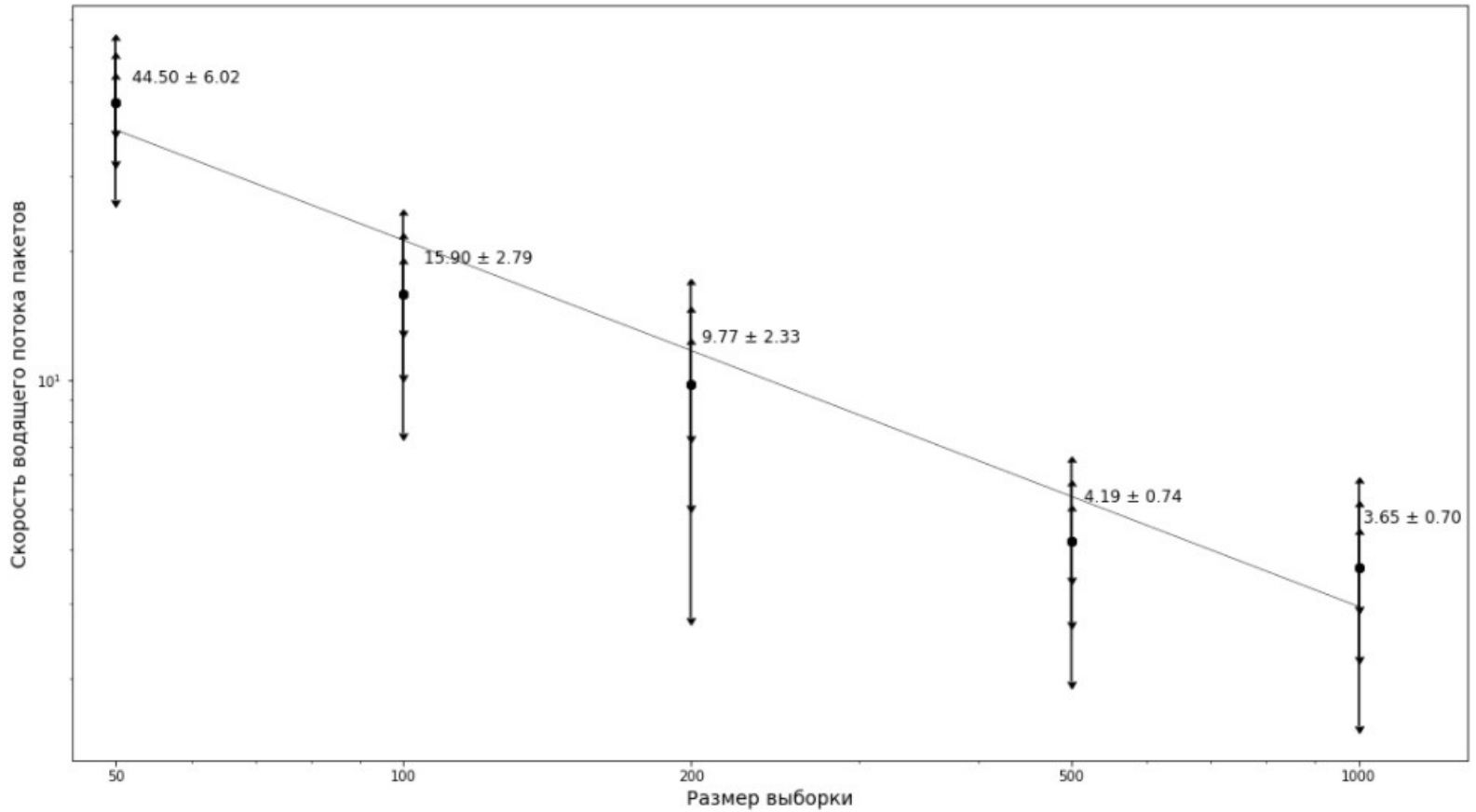
Временная зависимость для скорости входящего потока пакетов $B_N(t)$ при выборке «1 из 200»

Проверка гипотезы

Номер эксперимента	Разрешение N_k	Средняя скорость входящего потока пакетов B_k	Среднеквадратичное отклонение $\sigma(B_k)$	$B_k \cdot N_k$	$\sigma(B_k) \cdot N_k$
1	50	44,50	6,02	2225	301
2	100	15,90	2,79	1590	279
3	200	9,77	2,33	1954	466
4	500	4,19	0,74	2095	370
5	1000	3,65	0,70	3650	700

Данные о входящем трафике

Проверка гипотезы



Зависимость скорости входящего потока пакетов $B_N(t)$ от размера выборки N_i в логарифмических осях.

Результаты

- Найдена теоретическая зависимость порогового значения от величины выборки
- Найдено предельное разрешение выборки, при котором данное пороговое значение может быть обнаружено
- Разработана схема эксперимента по проверке теоретической гипотезы
- В ходе эксперимента подтверждена зависимость порогового значения от величины выборки

Контактная информация

Электронная почта:

Сухов Андрей Михайлович

Электронная почта:

amskh@yandex.ru

Телефон:

+7 927 785-67-48

ВКонтакте:

https://vk.com/id21428899

Сайт:

https://scholar.google.ru/citations?user=5wZKKcwAAAAJ