Ежегодная международная научно-практическая конференция
«РусКрипто'2025»

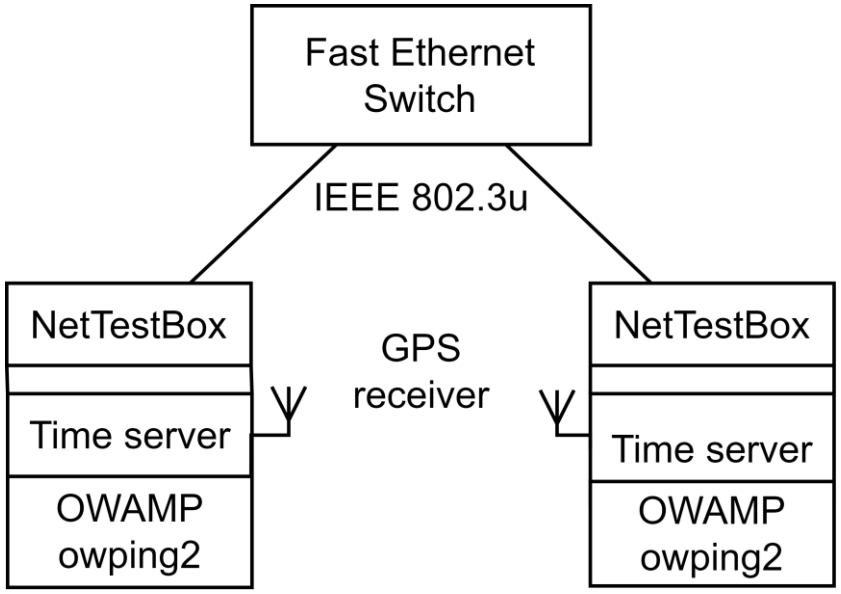
Определение аномальных сетевых состояний на основе измерений односторонней сетевой задержки

Сагатов Евгений Собирович, к.т.н., доцент, с.н.с, Самарский университет, sagatov@ya.ru
Черныш Дмитрий Петрович, старший преподаватель кафедры КИМ, Крымский федеральный университет, petrovka.net@gmail.com
Сухов Андрей Михайлович, д.т.н., профессор, Самарский университет, sukhov@ssau.ru

Сетевые атаки на переполнение канала

- DDOS- атаки трудно обнаружить и противостоять им
- Используют множество ботов для перегрузки сетевой инфраструктуры
- Могут привести к изменению сетевых маршрутов

Измерение односторонней сетевой задержки (OWD)



Измерение OWD в локальной сети с помощью платформы NetTestBox

- ***NetTestBox*** – универсальная платформа для измерения односторонней сетевой задержки
- Утилита **owping2** использует более точный механизм установки меток повышающий точность измерений
- Для синхронизации времени можно использовать приёмники сигнала GPS/GLONASS/BeiDou/Galileo

Функции распределения OWD для встречных направлений

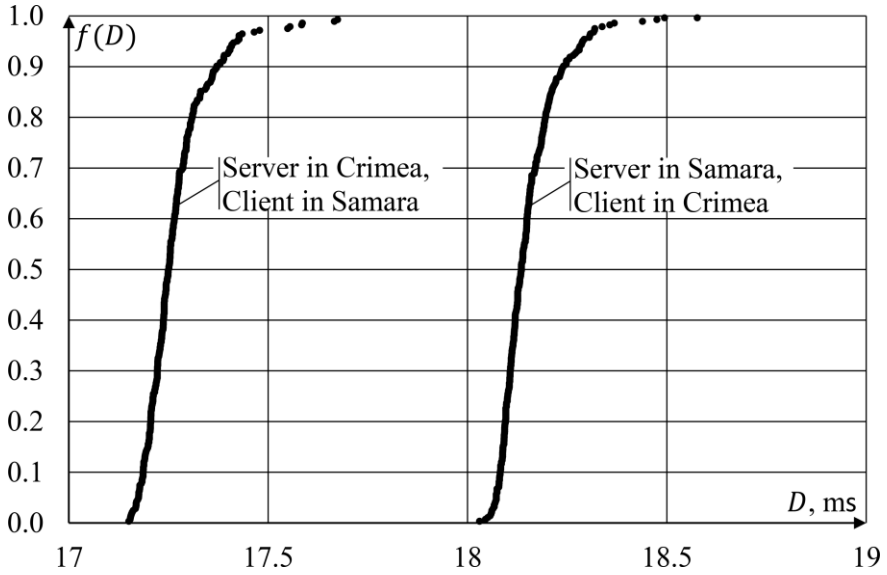


График функции распределения для OWD на участке Самара-Крым

Сравнительная характеристики функции распределения

Node location	D_{min}, ms	D_{avg}, ms	Jitter, ms
Client in Samara, server in Crimea	17.15	17.27	0.10
Client in Crimea, server in Samara	18.03	18.15	0.08

Экспериментальные измерения

Исходные данные

- Ширина интернет-канала – 100 Мбит/сек
- DDoS атака из внешней сети
- Постепенное увеличение мощности атаки
- Увеличение OWD при превышении ширины канала

Результат

- Увеличение значения OWD
- Рост джиттера
- Потери пакетов при превышении пропускной способности канала

Определение момента атаки

№	Attack power (*Mbps*)	OWD (ms) (*ms*)	Jitter (ms) (*ms*)	packet loss (%)
1	0	20,04	0,4	0
2	9	20,04	0,5	0
3	20	21,04	1,2	0
4	50	25,00	2,8	0
5	77	25,00	4,1	0
6	100	25,00	4,9	0
7	107	34,00	5,4	9,9

Характеристика OWD при увеличении мощности атаки на участке Самара - Крым

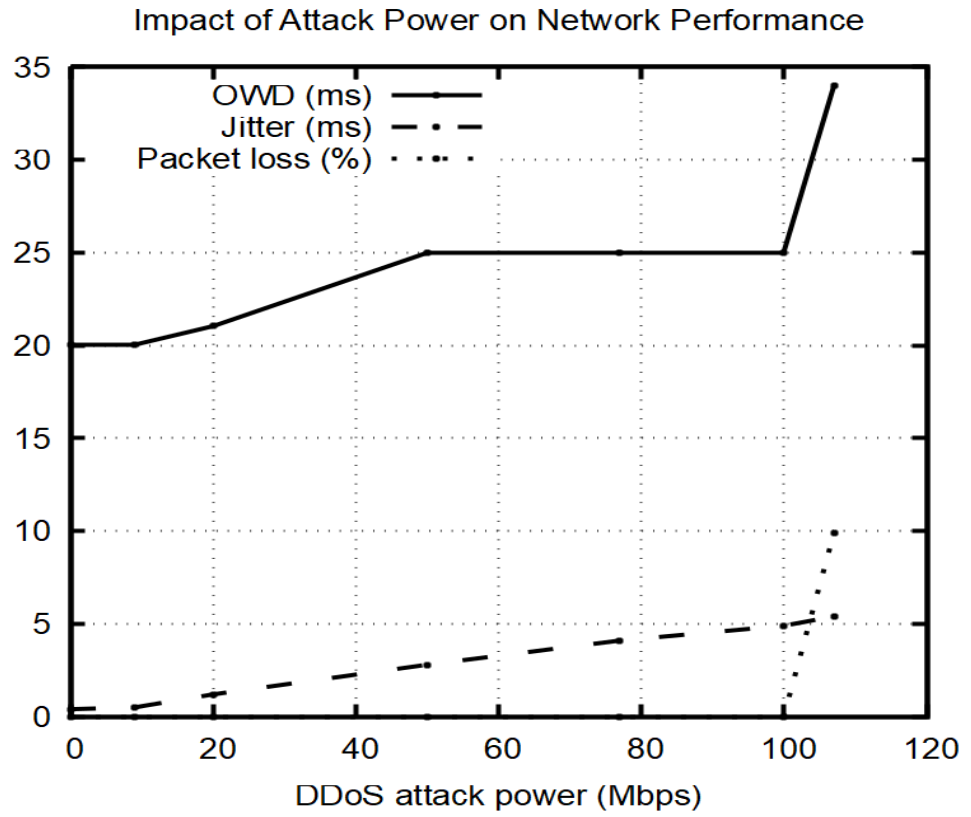
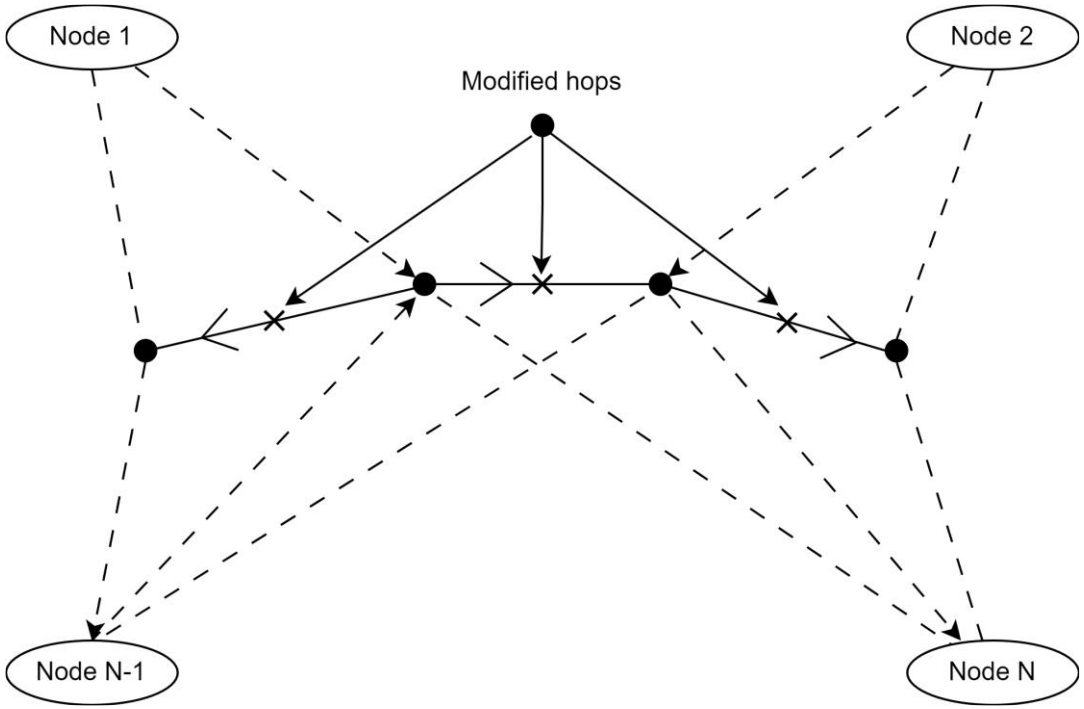


График зависимости характеристик OWD от мощности атаки на участке Самара - Крым

Смена маршрута как признак DDoS-атаки



Поиск замененных узлов маршрутизации

- Атаки могут приводить к перестроению маршрутов в сети.
- Изменение маршрута можно обнаружить практически мгновенно
- Возможно локализовать атакуемый участок сети

Помощь в исследовании

Исследование выполнено за счет гранта Российского научного фонда (проект № 24-29-00041)

Контактная информация

Электронная почта:

Сухов Андрей Михайлович

Электронная почта:

sukhov@ssau.ru

Телефон:

+7 927 785-67-48

ВКонтакте:

https://vk.com/id21428899

Сайт:

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