Моделирование противодействия бот-сетей и механизмов защиты от них

Коновалов А.М., **Шоров А.В.**

Аркадия, СПИИРАН

РусКрипто'2011, 30 марта - 2 апреля 2011 г.

Содержание

- Введение
- Этап распространения бот-сети
- Этап управления бот-сетью
- Этап реализации атак бот-сетью (атаки типа DDoS)
- Подход к моделированию
- Эксперименты
- Заключение

Введение

Защита от атак с использованием бот-сетей сегодня является очень актуальной проблемой.

Бот-сети активно применяются для рассылки спама, организации DDoS-атак, фишинга, удаленного перебора паролей и т.д. Чтобы обеспечить защиту от бот-сетей, необходимо исследовать методы их построения и функционирования, механизмы реализации атак с помощью бот-сетей, а также методы защиты от этих атак, в том числе методы обнаружения ботов.

Данная работа посвящена моделированию бот-сетей, этапов их функционирования и механизмов защиты, которые могут применяться на этих этапах.

Функционирование бот-сети

Функционирование бот-сетей характеризуется одновременными действиями большого количества бот-агентов в интересах злоумышленника.

Обычно функционирование бот-сети разделяют на следующие этапы:

- Этап распространения
- Этап управления
- Реализация атаки

Содержание

- Введение
- Этап распространения бот-сети
- Этап управления бот-сетью
- Этап реализации атаки бот-сетью (атаки типа DDoS)
- Подход к моделированию
- Эксперименты
- Заключение

Распространение бот-сети с помощью сетевого червя

Для распространения бот-сети исследовался метод распространения с помощью сетевого червя.

Параметры, определяющие механизм распространения сетевых червей:

- Тип соединения: TCP, UDP;
- Частота генерации пакетов;
- Изменение скорости сканирования;
- Тип сканирования (Scan type): случайное сканирование, последовательное сканирование, сканирование на основе перестановок, частичное сканирование, локальное сканирование, топологическое сканирование, сканирование по хит-листам.

Механизмы защиты от распространения сетевого червя

- Механизмы, основанные на “дросселировании/регулировании вирусов” (“virus throttling”) [Williamson, 2002]
- Механизмы, основанные на анализе неудачных соединений (Failed Connection) [Chen, Tang,2007]
- Механизмы, основанные на методе “порогового случайного прохождения” (Threshold Random Walk) [Nagaonkar , Mchugh, 2008]
- Механизмы ограничения интенсивности соединений на основе кредитов доверия (Credit Base-based Rate Limiting)

Содержание

- Введение
- Этап распространения бот-сети
- Этап управления бот-сетью
- Этап реализации атаки бот-сетью (атаки типа DDoS)
- Подход к моделированию
- Эксперименты
- Заключение

Модель управления бот-сетью

Исследовались две архитектуры для управления бот-сетью: с централизованным управлением и децентрализованным управлением.

- В случае централизованного управления все компьютеры-«зомби» соединяются с одним командным центром (Command & Control Center).
- При децентрализованном управлении, боты соединяются не с центром управления, а с несколькими зараженными машинами из бот-сети. Команды, в этом случае, передаются от бота к боту

Обнаружение компьютеров-«зомби» на фазе управления

- Метод на основе анализа кооперативного поведения бот-агентов (Proposal of metrics for botnet detection based on its cooperative behavior) [Akiyama et al., 2007]
- Метод обнаружения бот-сетей, основанный на их поведении (Botnet Detection Based on Network Behavior) [Strayer et al., 2008]
- Метод, основанный на обнаружении аномалий производимых бот-сетями (Algorithm for Anomaly-based Botnet Detection) [Binkley, Singh, 2006]

Содержание

- Введение
- Этап распространения бот-сети
- Этап управления бот-сетью
- Этап реализации атаки бот-сетью (атаки типа DDoS)
- Подход к моделированию
- Эксперименты
- Заключение

Методы реализации DDoS-атак

Исследовались следующие типы атак DDoS:

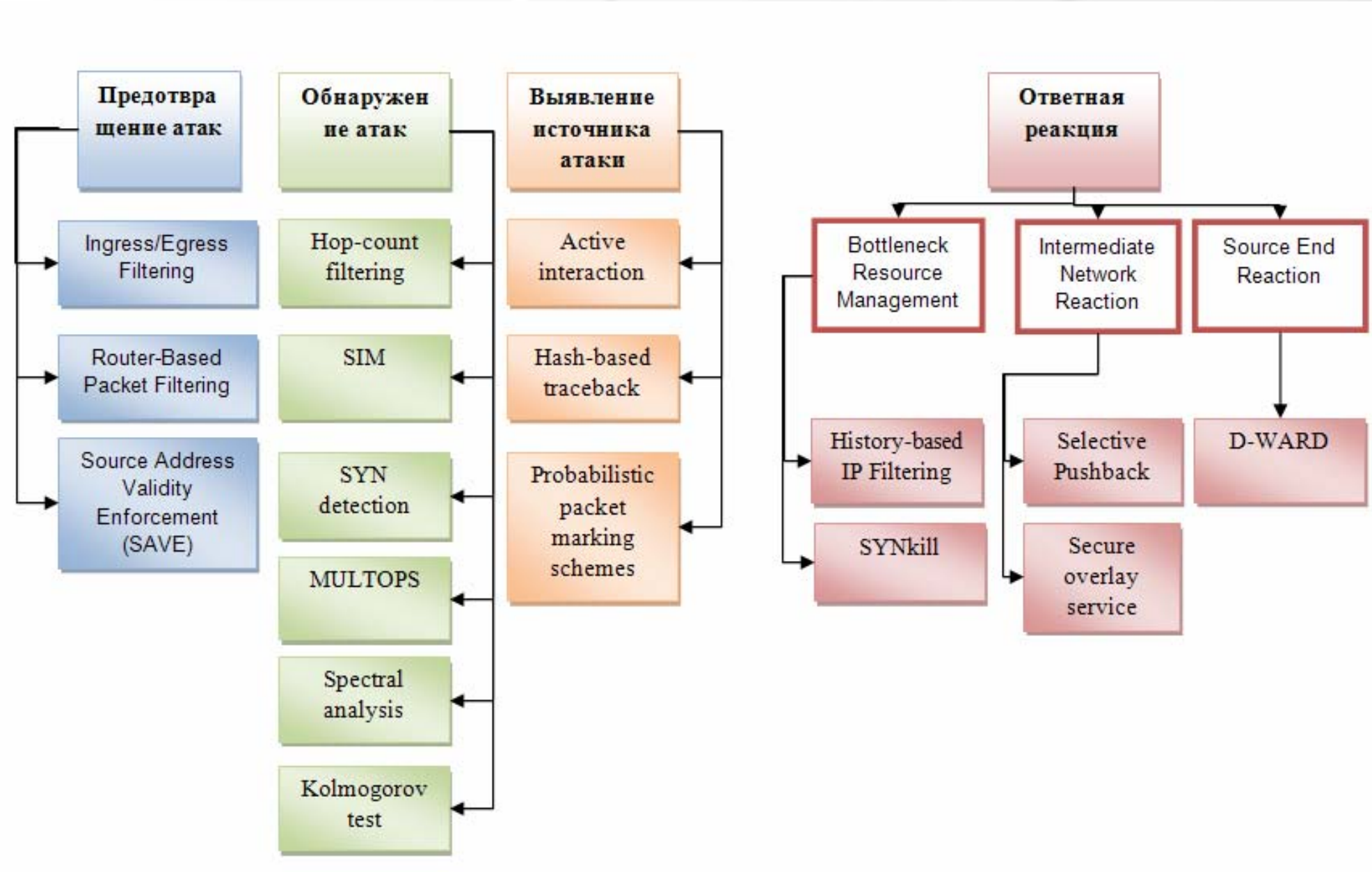
- Атаки на исчерпание ресурсов, используя транспортные протоколы (SYN Flood, ICMP Flood, Smurf, UDP-storm, Fraggle, Land).
- Атаки на исчерпание ресурсов, используя прикладные протоколы (HTTP Flood, SIP Flood)
- Атаки DDoS с использованием третьих лиц (DRDoS - Distributed Reflector Attacks).

Защита от DDoS-атак

Как правило, есть четыре основных этапа по противодействию DDoS-атакам:

- предотвращение атак,
- обнаружение атак,
- выявление источника нападения,
- реакция на атаку.

Методы защиты от DDoS-атак



Содержание

- Введение
- Этап распространения бот-сети
- Этап управления бот-сетью
- Этап реализации атаки бот-сетью (атаки типа DDoS)
- Подход к моделированию
- Эксперименты
- Заключение

Архитектура программной реализации модели

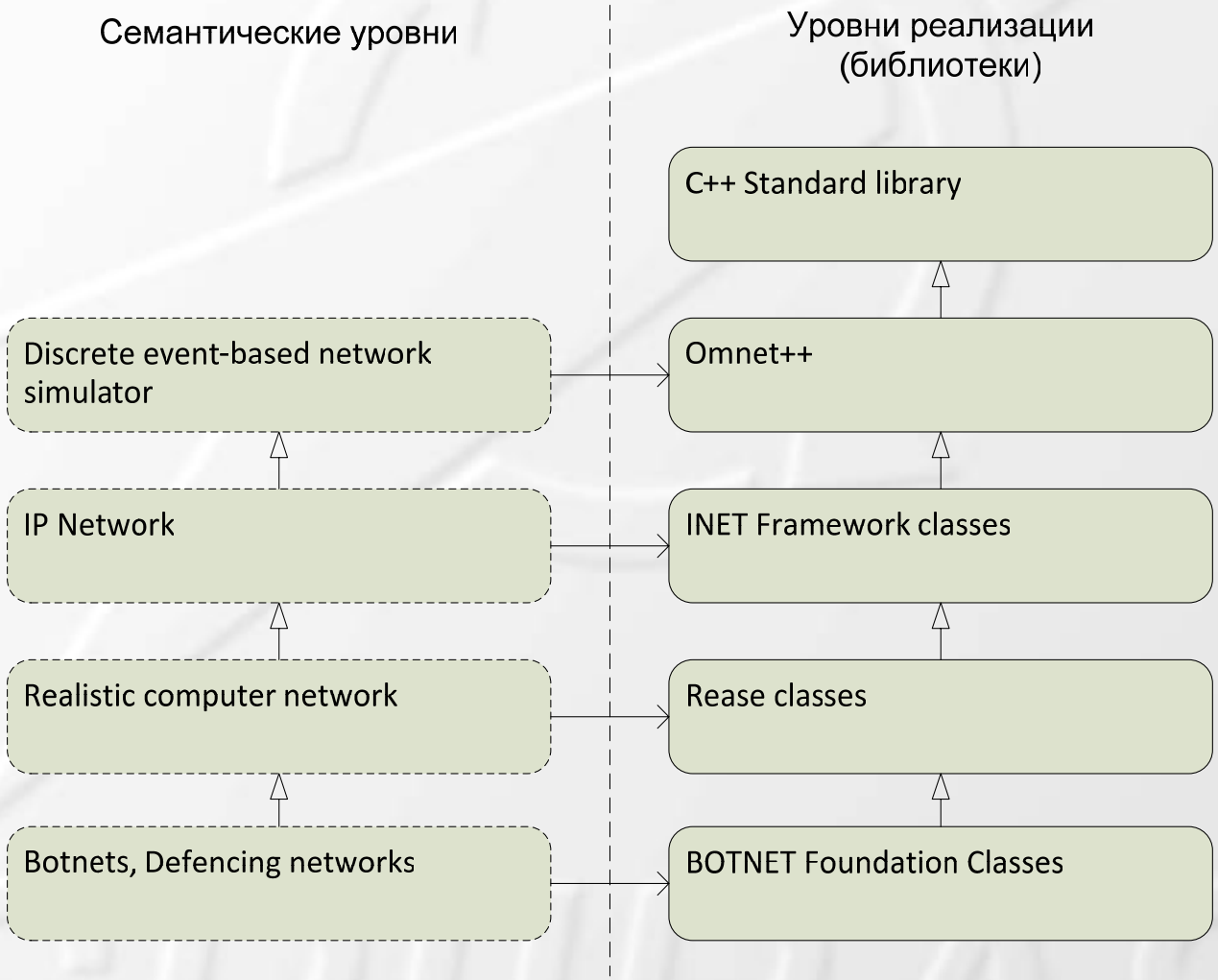


Диаграмма использования компонент среды моделирования

Модели распространения сетевых червей и защиты от них, реализованные в OMNeT++

В настоящее время с помощью системы имитационного моделирования OMNeT++ реализованы следующие модели распространения сетевых червей защиты от них:

- Модели распространения червей: Code Red II, Sasser. Множество настраиваемых параметров позволяют моделировать большое количество червей, работающих по протоколу TCP.
- Механизмы защиты, основанные на “дросселировании/регулировании вирусов” (Virus Throttling), анализе неудачных соединений (Failed Connection).

Модели управления бот-сетями и их обнаружения, реализованные в OMNeT++

- Построена модель архитектуры бот-сети с централизованным управлением.
- Были реализованы отдельные методы кооперативного обнаружения бот-агентов.

Модели DDoS-атак и защиты от них, реализованные в OMNeT++

Для выполнения DDoS-атак и защиты от них в OMNeT++ реализованы следующие модели:

- Механизмы выполнения DDoS-атак на уровне транспортных протоколов.
- Механизмы защиты от DDoS-атак, основанные на: SAVE, SIM, Hop-count filtering.

Модели имеют ряд настраиваемых параметров, позволяющих имитировать работу механизмов DDoS-атак и защиты от них.

С помощью построенных моделей проводятся различные эксперименты.

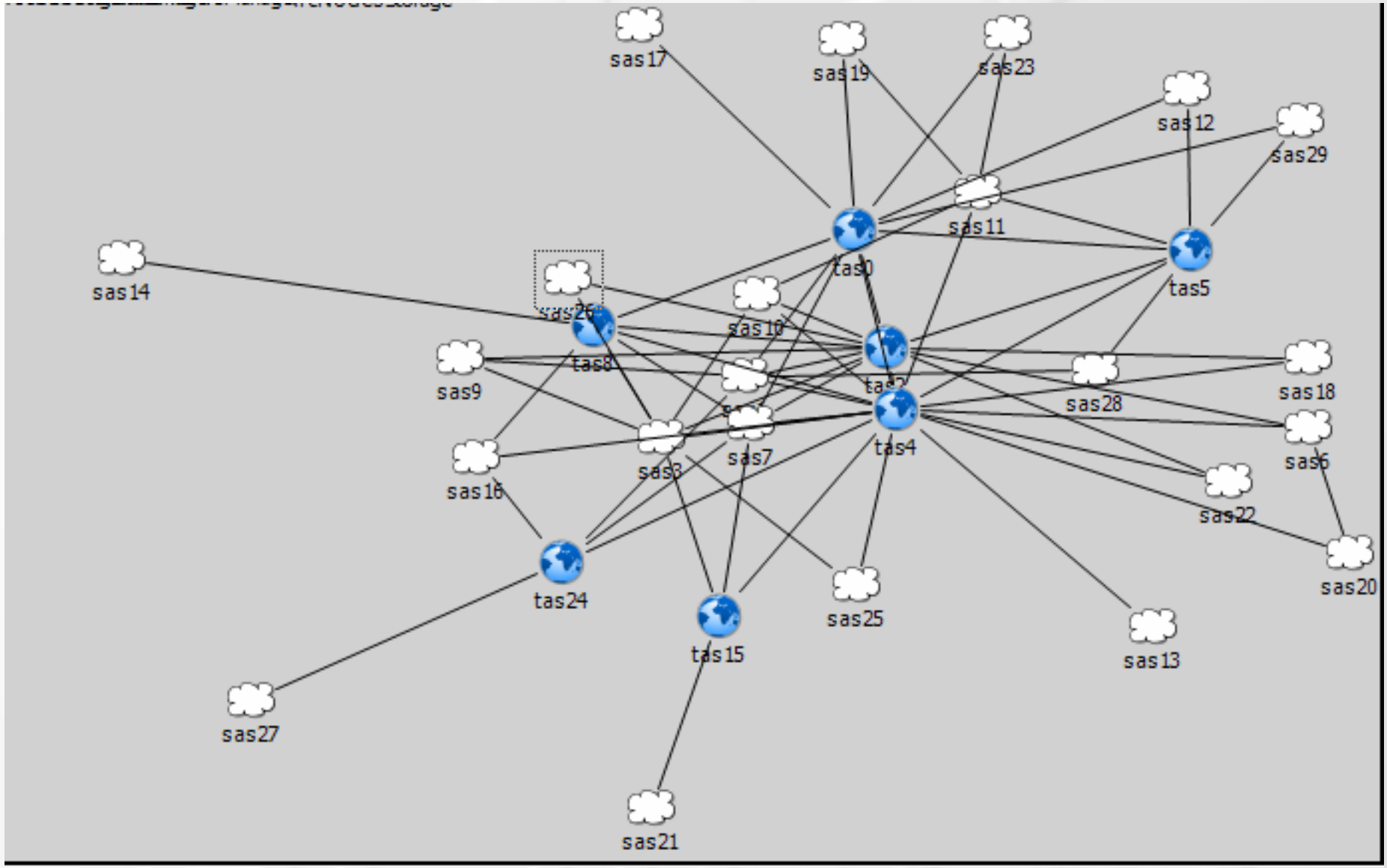
Содержание

- Введение
- Этап распространения бот-сети
- Этап управления бот-сетью
- Этап реализации атаки бот-сетью (атаки типа DDoS)
- Подход к моделированию
- Эксперименты
- Заключение

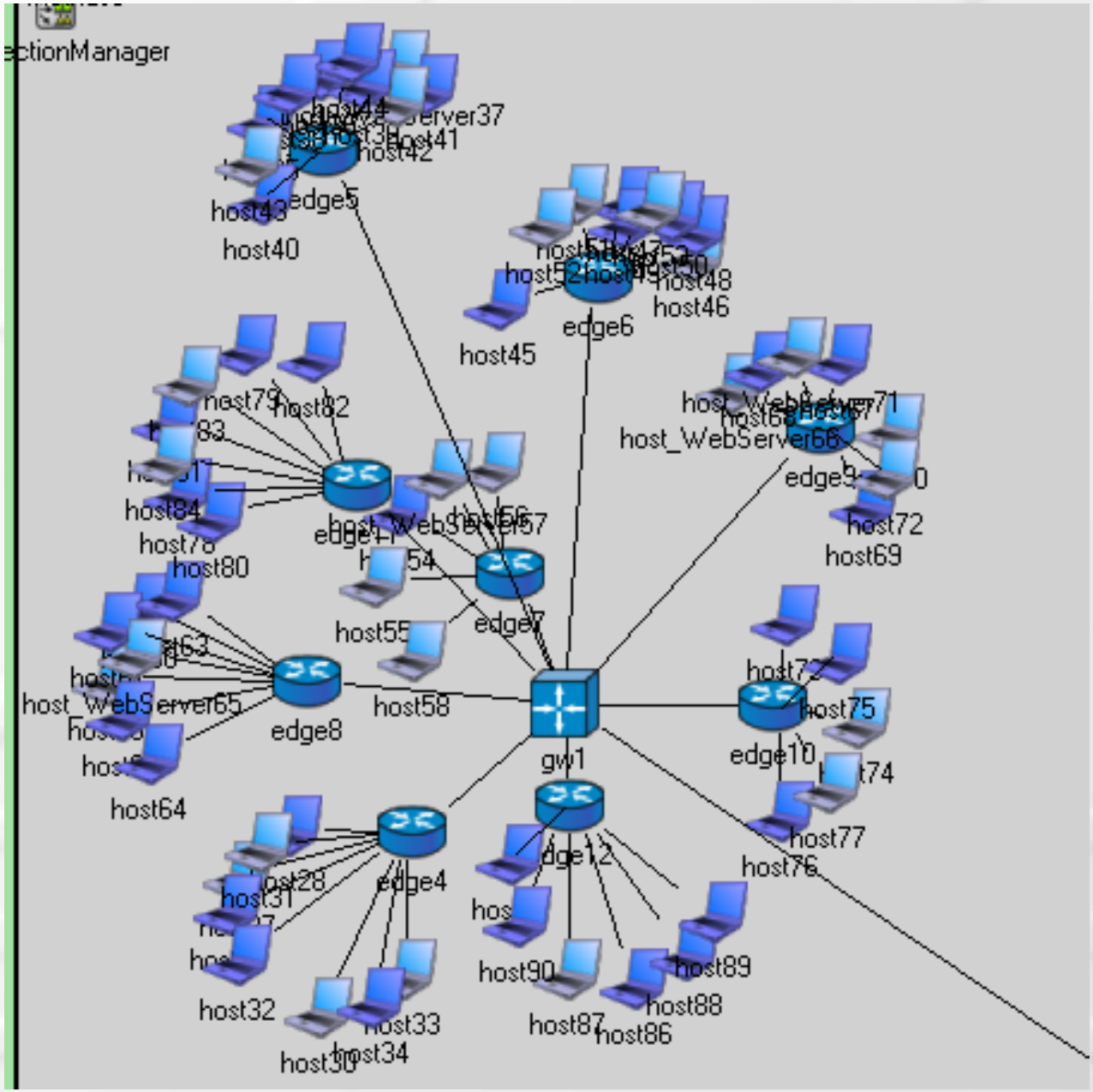
Эксперименты

Для проведения экспериментов построена модель компьютерной сети на 3652 узлов, из которых 10 являются серверными узлами, в состав которых входят DNS-сервера — 1, веб-сервера — 3, почтовые сервера — 6. 1119 узлов (около 30% от общего количества) имеют уязвимости.

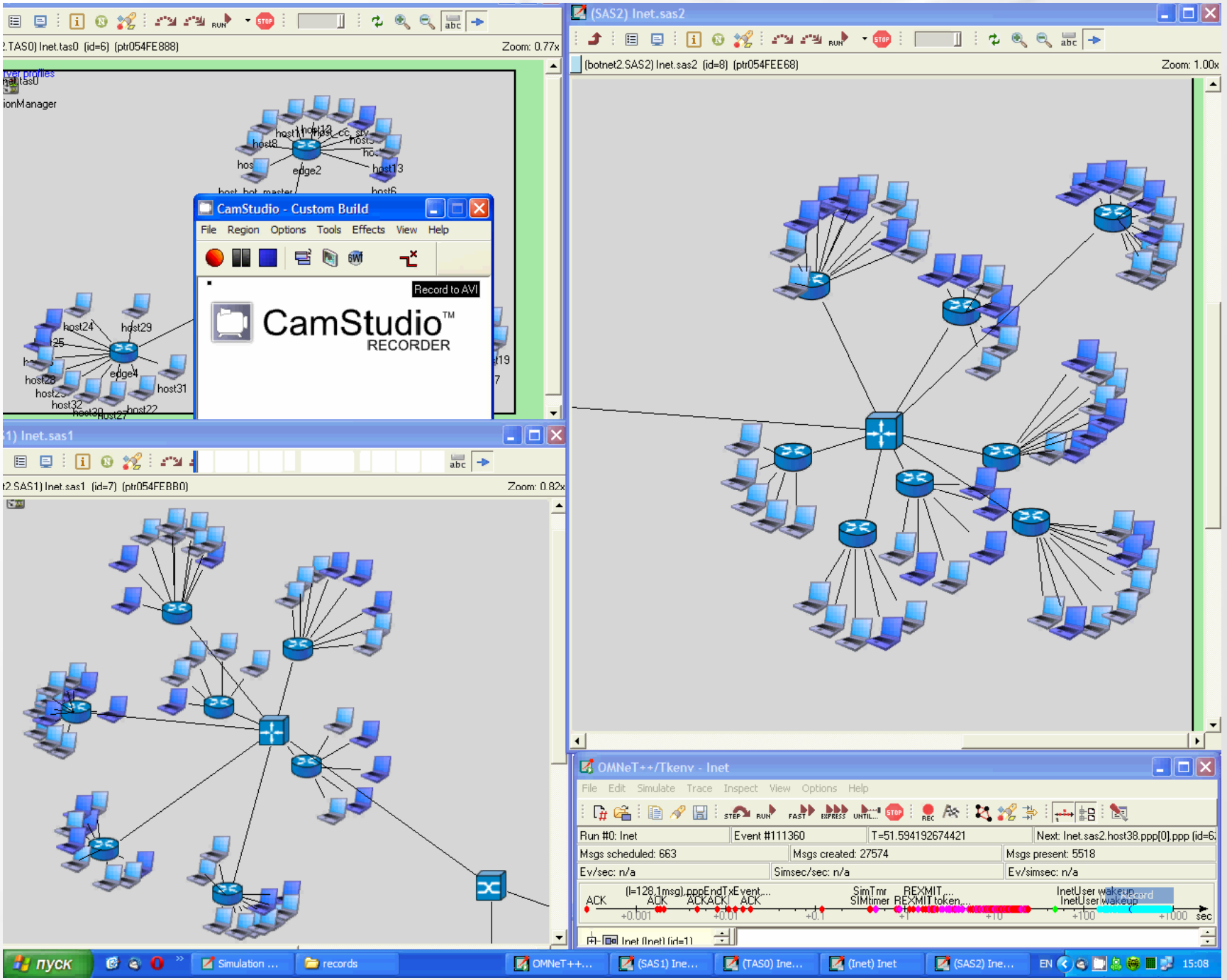
Модель сети


sas17
sas19
sas23
sas12
sas29
sas11
sas14
tas0
tas5
sas26
sas10
tas8
sas9
sas18
sas28
sas6
sas16
sas3
sas7
tas4
sas22
sas20
tas24
sas25
tas15
sas13
sas27
sas21

Нижний уровень модели сети



Пример работы модели



Моделирование распространения червя и механизмов защиты от них

- Распространение червя начиналось на 100 секунде модельного времени.
- Использовался алгоритм случайного сканирования из диапазона известных адресов со скоростью 6 запросов в секунду, по протоколу TCP/IP.
- Использовались модели механизмов защиты на основе Failed Connection и Virus Throttling, установленные на 100% маршрутизаторов сети.

График количества ошибок первого и второго рода при обработке сетевых пакетов механизмом на основе Virus Throttling, установленного на 50% маршрутизаторов

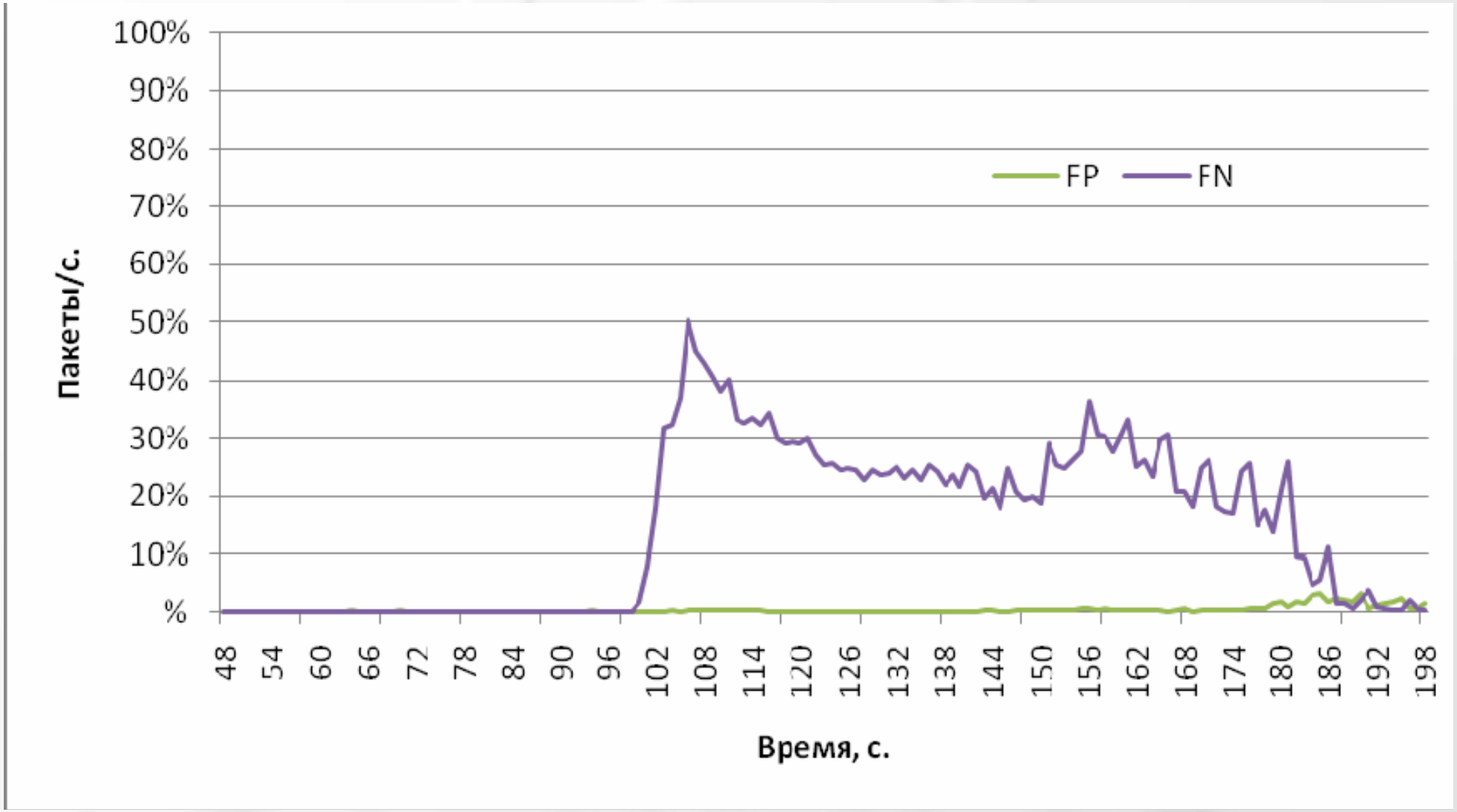
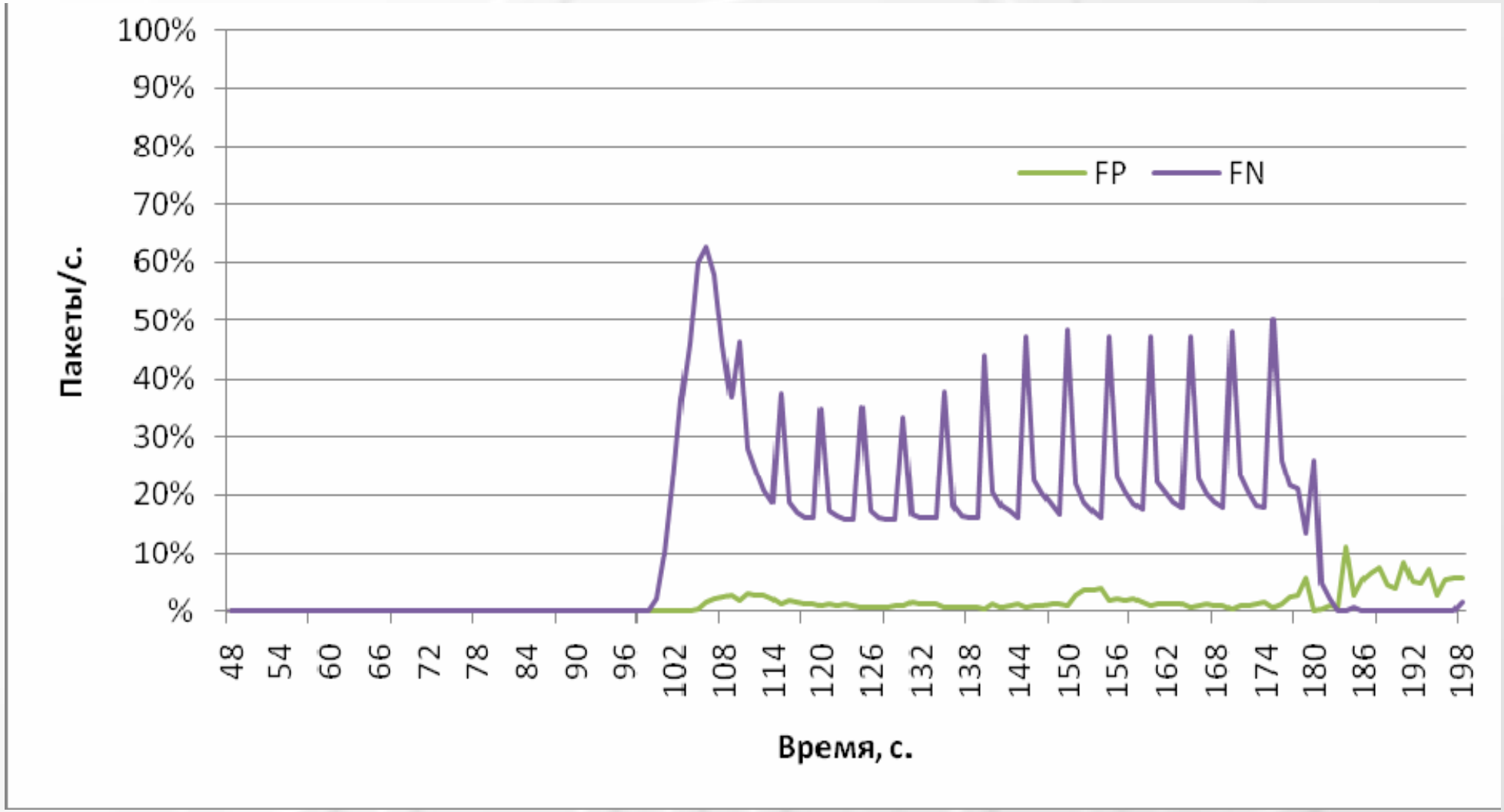
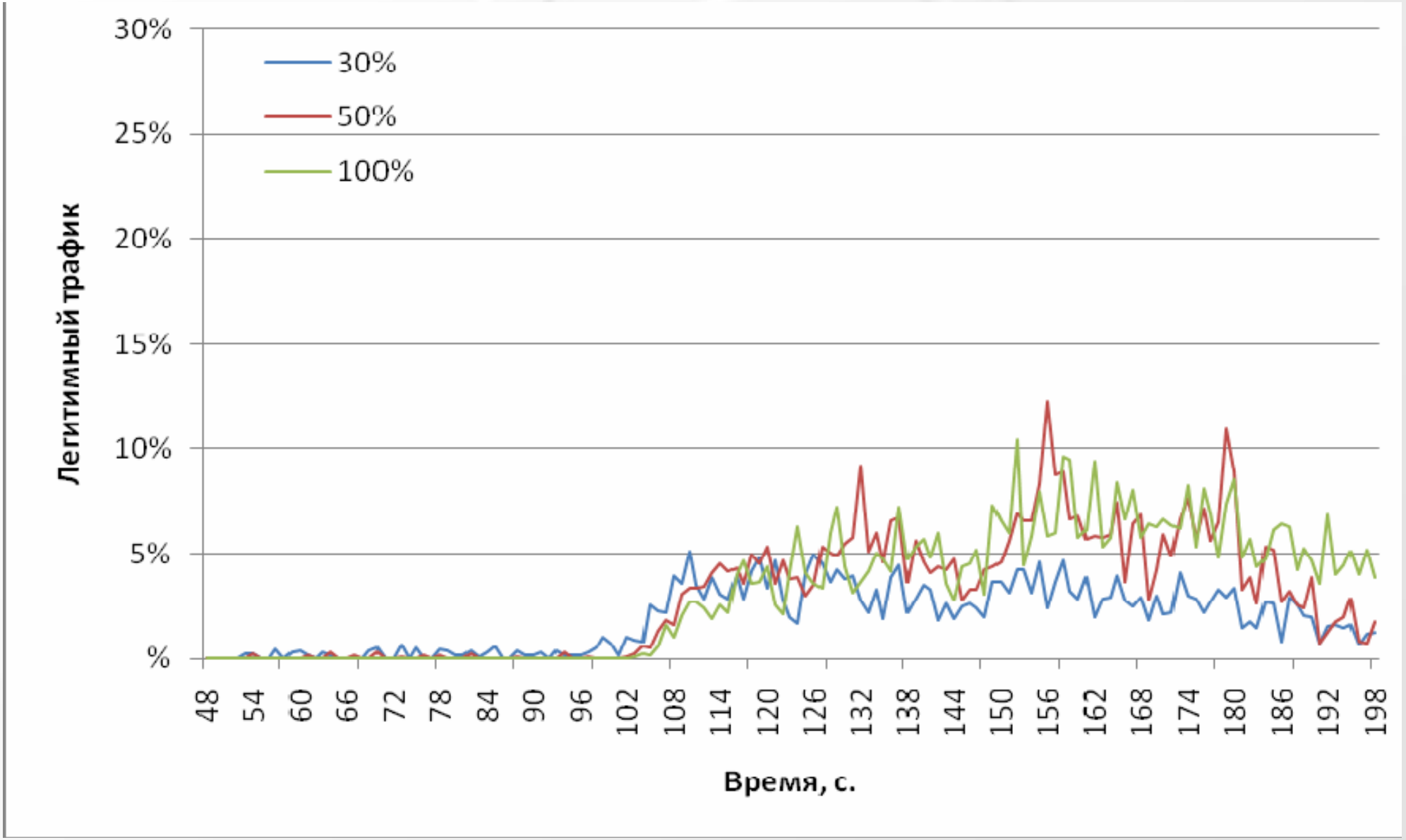


График количества ошибок первого и второго рода при обработке сетевых пакетов механизмом на основе Failed Connection, установленного на 50% маршрутизаторов



Отношение фильтрованного легитимного трафика к общему легитимному трафику при работе механизма защиты, основанного на Virus Throttling



Моделирование фазы управления бот-сетью с использованием протокола IRC и механизмов ее обнаружения

- Для коммуникации между компьютерами- «зомби», командным центром и «мастером» используется модель протокола на основе протокола IRC.
- Для обнаружения узлов бот-сети на этапе управления используется метод на основе [Akiyama et al., 2007].

Распределение участников по IRC-каналам

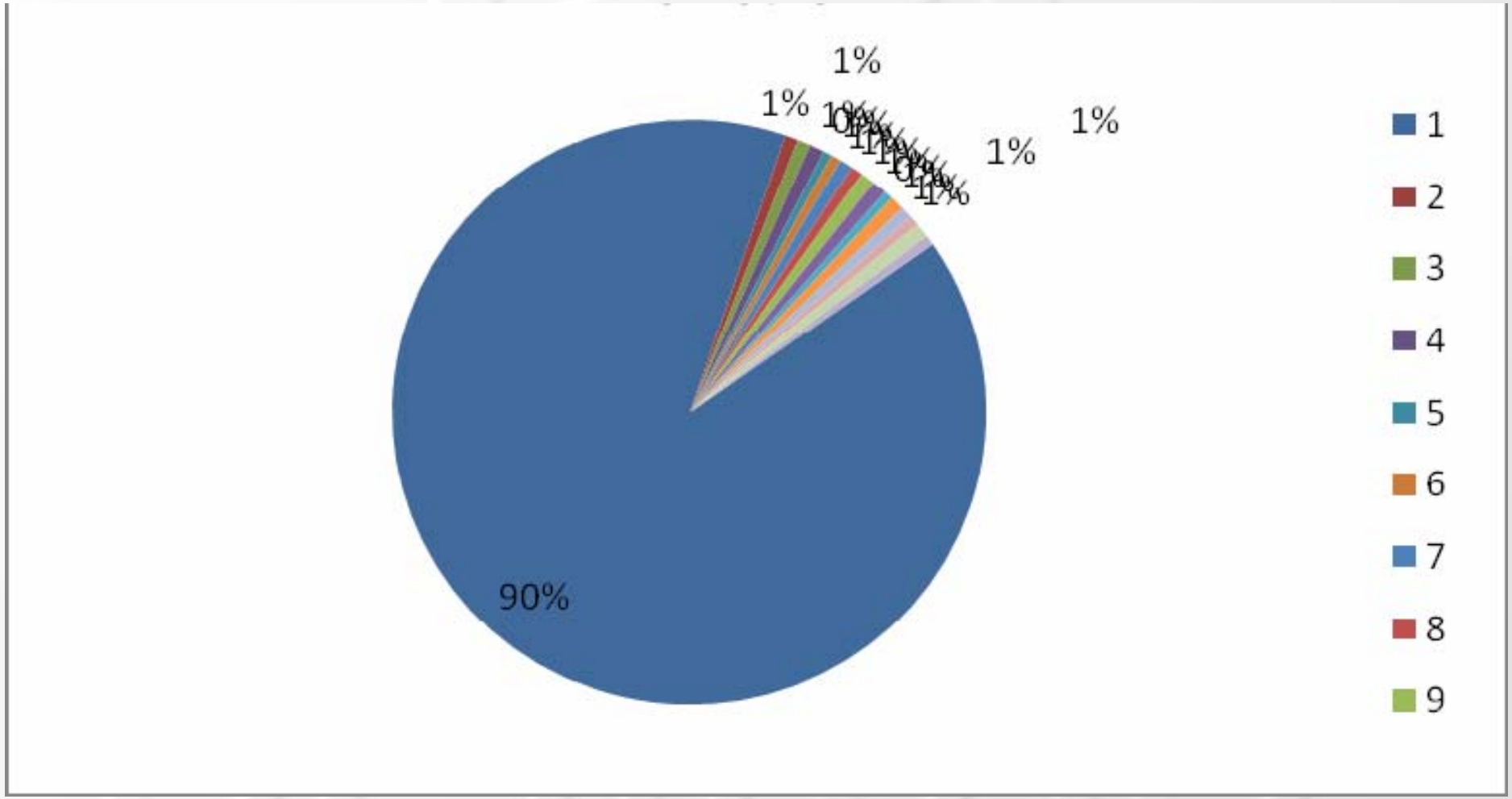
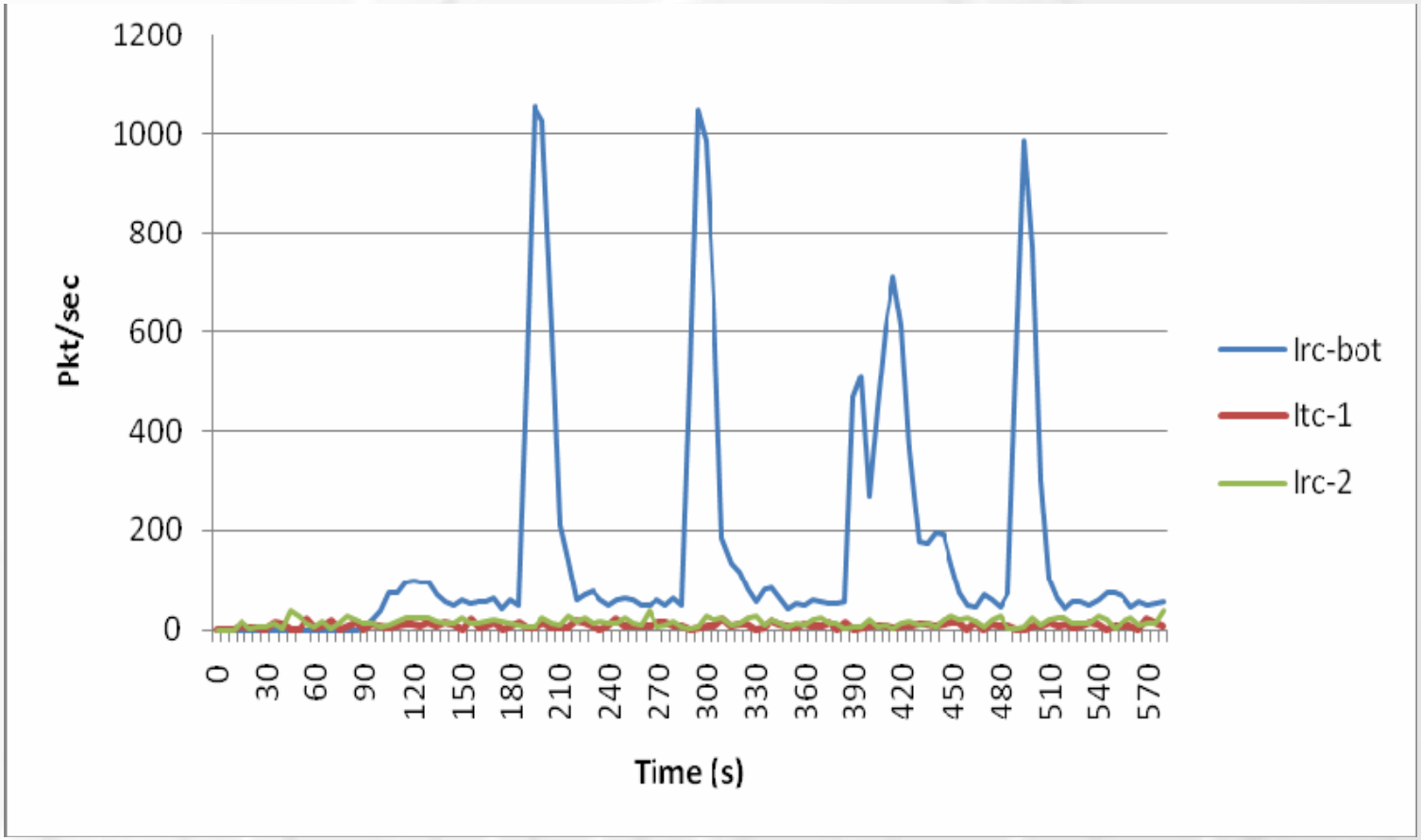


График обнаружения аномалий в IRC-трафике



Количество IRC пакетов в секунду, относящихся к различным IRC каналам, измеренное детектором в различных точках сети

Моделирование фазы выполнения DDoS-атаки бот-сетью и механизмов защиты от них

- Выполнялась DDoS-атака типа SYN-flooding. Атака начиналась на 400 с. модельного времени. Пакеты отсылались с частотой 10 пакетов в секунду, выполнялась подмена IP-адреса источника.
- Для защиты от DDoS-атаки использовались механизмы защиты на основе SAVE и SIM.
- Механизм на основе SAVE был установлен на 30%, 50%, 100% маршрутизаторов в сети
- Порог появления новых IP в секунду равен 600.

График на основе данных, полученных в результате выполнения моделей механизмов DDoS-атак и механизма защиты на основе SAVE

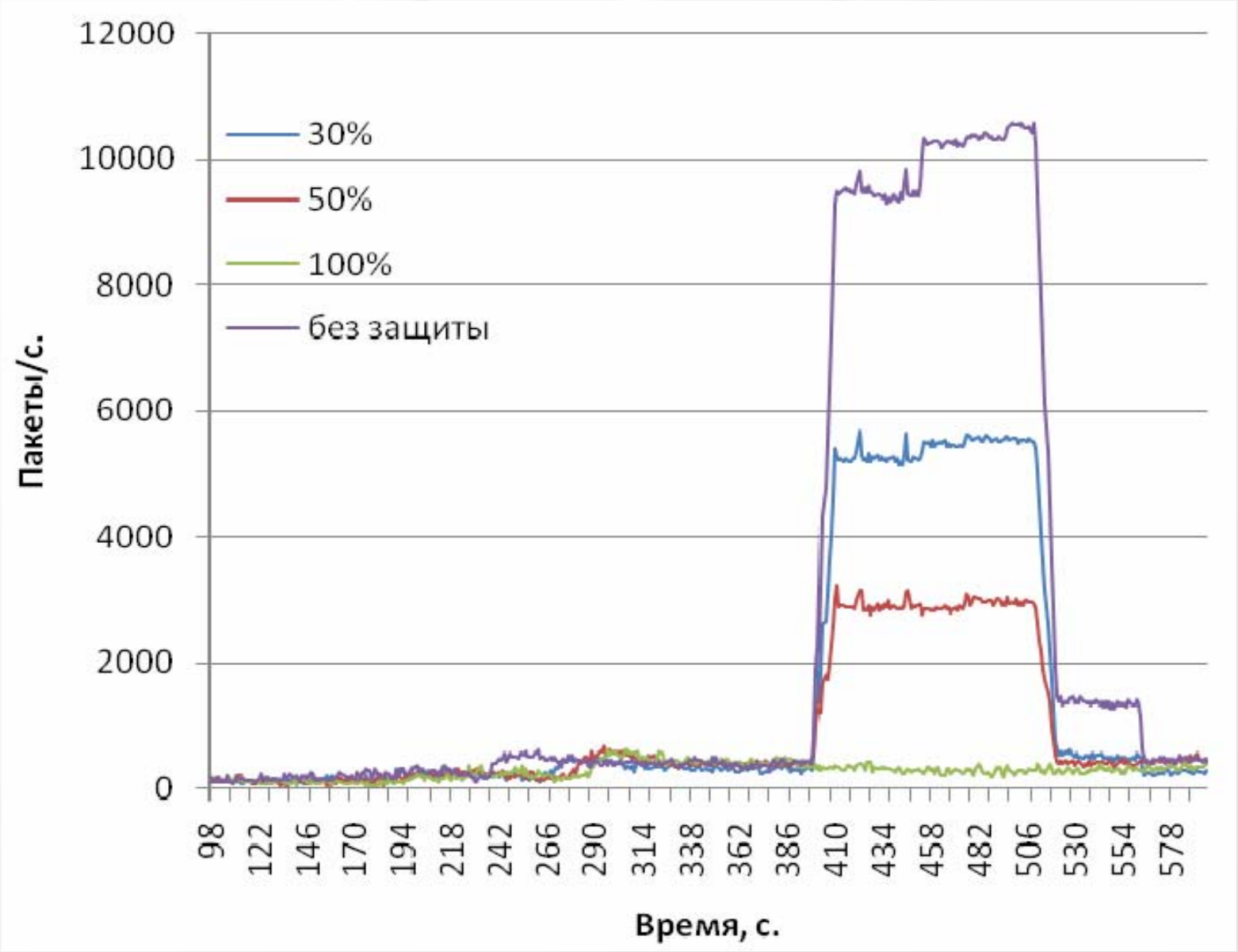
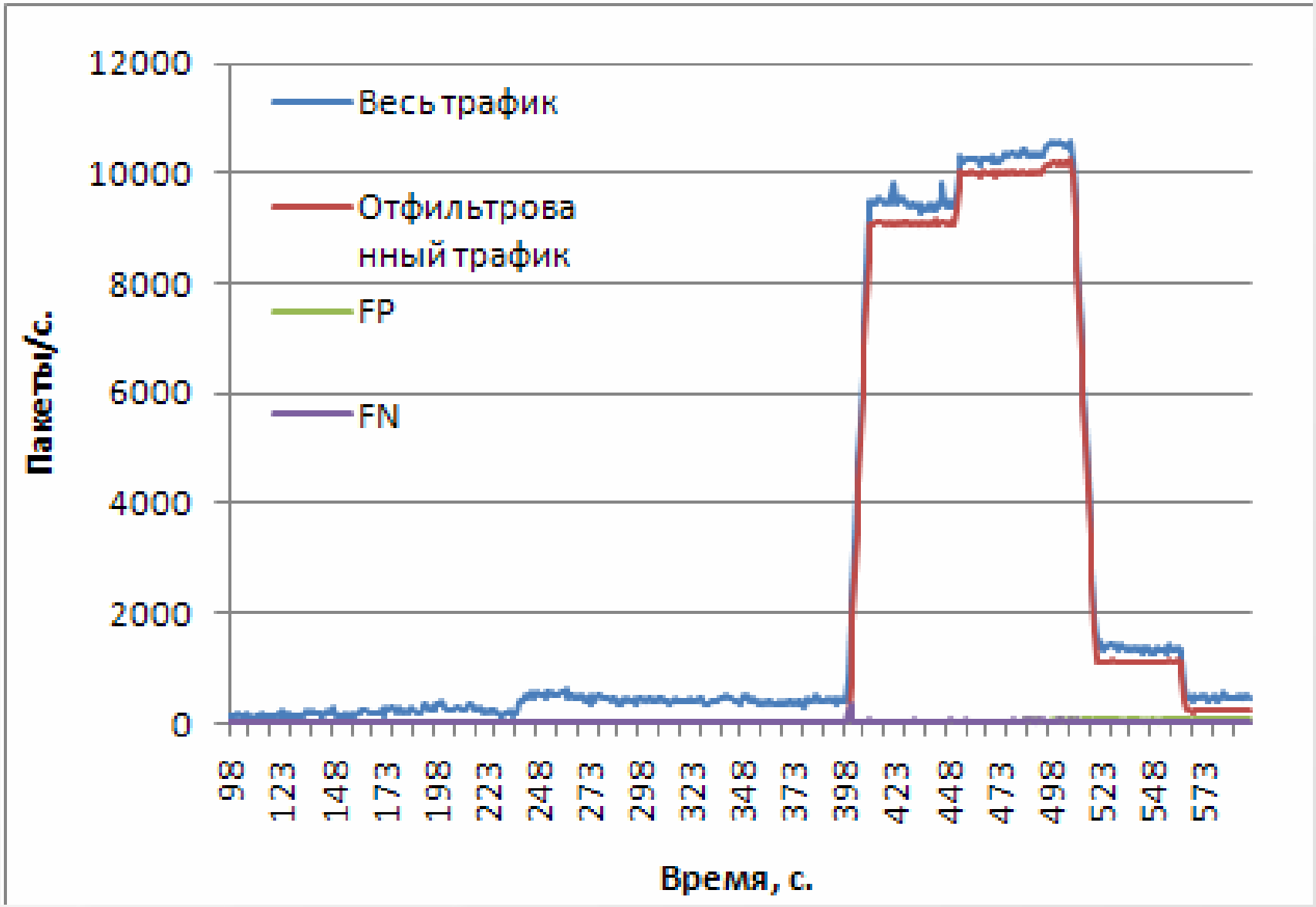


График на основе данных, полученных в результате выполнения моделей механизмов DDoS-атак и механизма защиты на основе SIM



Заключение

- В настоящей работе проведен анализ различных этапов функционирования бот-сети и механизмов защиты от них.
- Предложена архитектура среды моделирования, разработаны имитационные модели, выполняющие различные этапы функционирования бот-сетей в данной среде.
- Приведены результаты экспериментов по функционированию бот-сетей и работе методов защиты от них.

Контактная информация

Коновалов Алексей Михайлович

alexonline@hotbox.ru

Шоров Андрей Владимирович

ashorov@comsec.spb.ru

http://comsec.spb.ru/shorov/

Благодарности

Работа выполняется при финансовой поддержке РФФИ (проект 10-01-00826-а), программы фундаментальных исследований ОНИТ РАН (проект 3.2) и при частичной финансовой поддержке, осуществляемой в рамках проектов Евросоюза SecFutur и MASSIF.