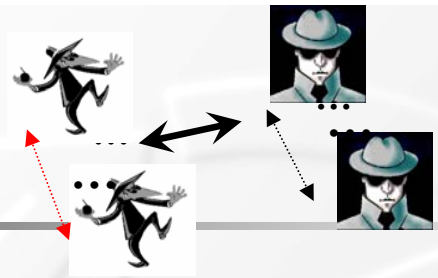


ИССЛЕДОВАНИЕ МЕХАНИЗМОВ ЗАЩИТЫ ОТ АТАК DDOS: ИМИТАЦИЯ ПРОТИВОБОРСТВА ИНТЕЛЛЕКТУАЛЬНЫХ АГЕНТОВ В СЕТИ ИНТЕРНЕТ

И.В. Котенко, А.В. Уланов

НИГ компьютерной безопасности
Санкт-Петербургский институт информатики и автоматизации РАН

«РусКрипто'2008», 3 - 6 апреля 2008 г.

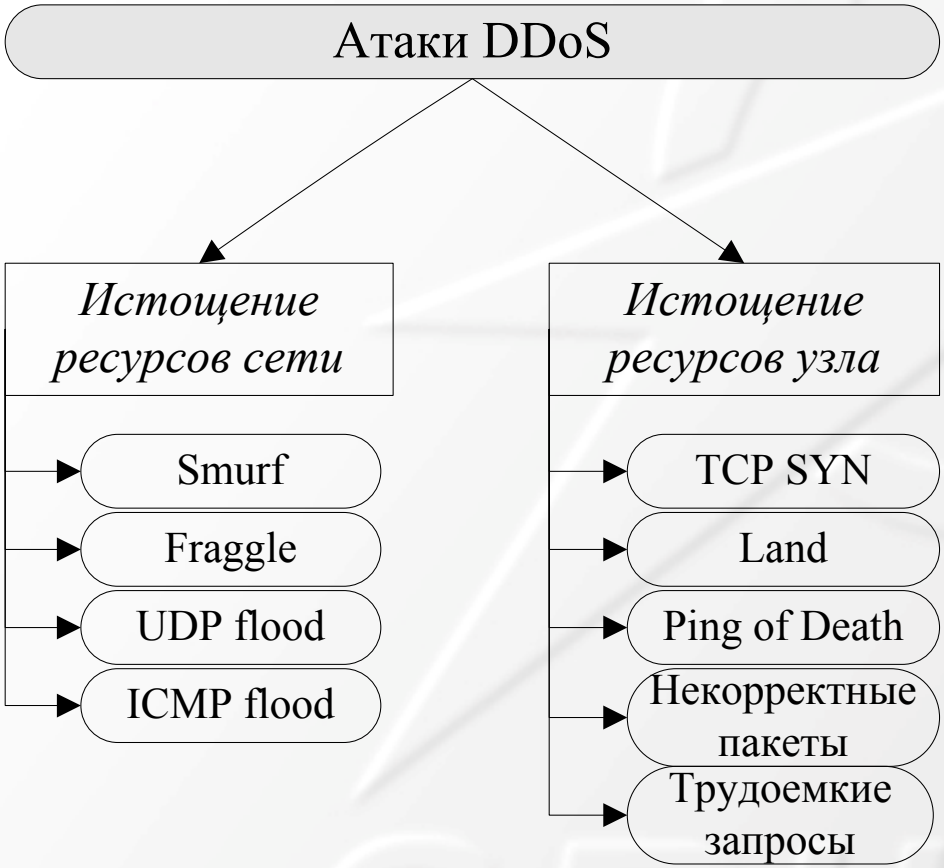
План доклада

- Введение
- Атаки DDoS и механизмы защиты
- Подход к моделированию
- Среда моделирования
- Эксперименты
- Заключение

Обоснование проблемы

- **Цель работы:** *разработка общего подхода и инструментальной среды для многоагентного моделирования противоборства команд программных агентов в компьютерных сетях (на примере DDoS-атак и механизмов защиты от них).*
- **Теоретические задачи:** исследование новых механизмов защиты
- **Прикладные задачи:** оценка безопасности существующих сетей, рекомендации по построению перспективных систем защиты

Атаки DDoS



- DDoS – Distributed Denial of Service – распределенный отказ в обслуживании

- Реализация атак DDoS: выход из строя хостов, служб, сегментов сети

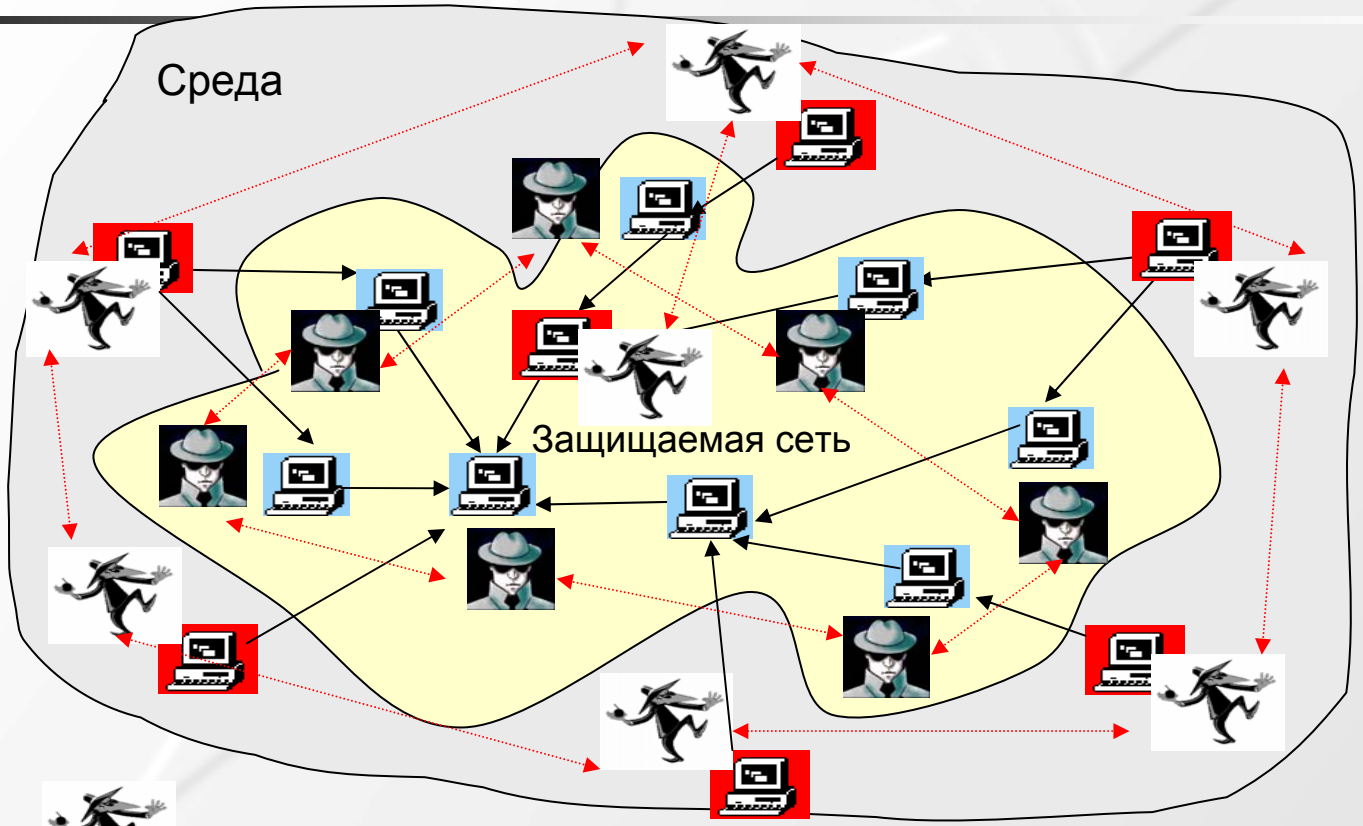
Механизмы защиты от DDoS атак

- Общий подход к защите от DDoS атак:
  - сбор информации о нормальном трафике
  - сравнение текущего трафика с модельным
  - прослеживание источников аномалий и выдача рекомендаций
  - применение выбранных контрмер

Кооперативные механизмы защиты от DDoS атак

- **Управление ресурсами**
  - Server Roaming
  - Market-based Service Quality Differentiation
  - Transport-aware IP router architecture
- **Аутентификация**
  - Transport-aware IP router architecture
  - Secure Overlay Services
- **Механизмы отслеживания (traceback)**
  - ACC pushback
  - COSSACK
  - Perimeter-based DDoS defense
  - DefCOM
  - Gateway-based

Многоагентное моделирование киберпротивоборства



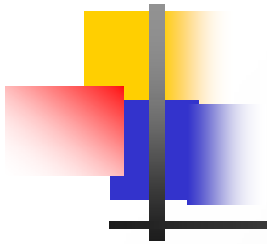
… - Команда агентов-злоумышленников

- Взаимодействие агентов-злоумышленников

- Маршрут атаки

… - Команда агентов защиты

- Взаимодействие агентов защиты



Основные работы, используемые в качестве базиса для исследований

- **Агентно-ориентированное моделирование**: N.Jennings, M.Wooldridge и др.
- **Командная работа агентов**: P.Cohen (общие намерения), B.Grosz, S.Kraus (разделяемые планы); M.Tambe (комбинированные подходы) и др.
- **Системы вывода, основанные на предсказании намерений и планов оппонента**: E.Charniak (формулировка задачи распознавания как задачи абдуктивного вывода); H.Kautz, J.Allen (распознавание плана на основе идентификации минимального множества высокоуровневых действий, которые достаточны для объяснения наблюдаемых действий) и др.
- **рефлексивные процессы**: В.А.Лефевр, В.Е.Лепский, Д.А.Поспелов и др.
- **теоретико-игровое моделирование**: J.Nash, G.Zlotkin , J.Rosenschtein, T.Sandholm, Ю.Б. Гермейер, А.И.Кондратьев и др.
- **Системы кооперативных распределенных грамматик** и грамматические модели агентских систем: M.ter Beek, J.Gaso, J.Kelemen, J.Dassow и др.
- **Моделирование атак на компьютерные сети:** [Ritchey *et al*-00], [Swiler *et al*-01], [Ortalo *et al*-01], [Sheyner *et al*-02] и др.
- **Моделирование процессов защиты информации**, в т.ч. моделей аутентификации и разграничения доступа, виртуальных частных сетей, инфраструктуры открытых ключей, обнаружения вторжений и др.

Работы в области многоагентного моделирования

- Классические подходы:
  - Теория общих намерений [Cohen 1991]
  - Теория общих планов [Grosz 1996]
  - Комбинированный подход, система Steam [Tambe 1997]
- Системы многоагентоного моделирования
  - GRATE*: общая ответственность [Jennings 1995]
  - OAA: доска объявлений [Martin 1999]
  - CAST: общая ментальная модель [Yen 2003]
  - RETSINA-MAS: комбинации всевозможных ролей агентов [Giampapa 2002]
  - Robocup soccer: ориентация на собственную модель мира [Stankevich 1999]
  - COGNET/BATON: взаимодействие людей и агентов [Zachary 1996]
  - Team-Soar: «многоуровневая теория» [Kang 2001]

Предлагаемый подход

- Кибернетическое противоборство представляется в виде взаимодействия различных команд программных агентов
- Процессы происходят в среде, задаваемой моделью Интернета
- Выделяются команды агентов атаки и защиты
- Знания о предметной области содержатся в онтологиях
- Агенты взаимодействуют по протоколам и в соответствии со сценариями
- Команды взаимодействуют между собой: противоборствуют, кооперируются, адаптируются

Основные положения подхода

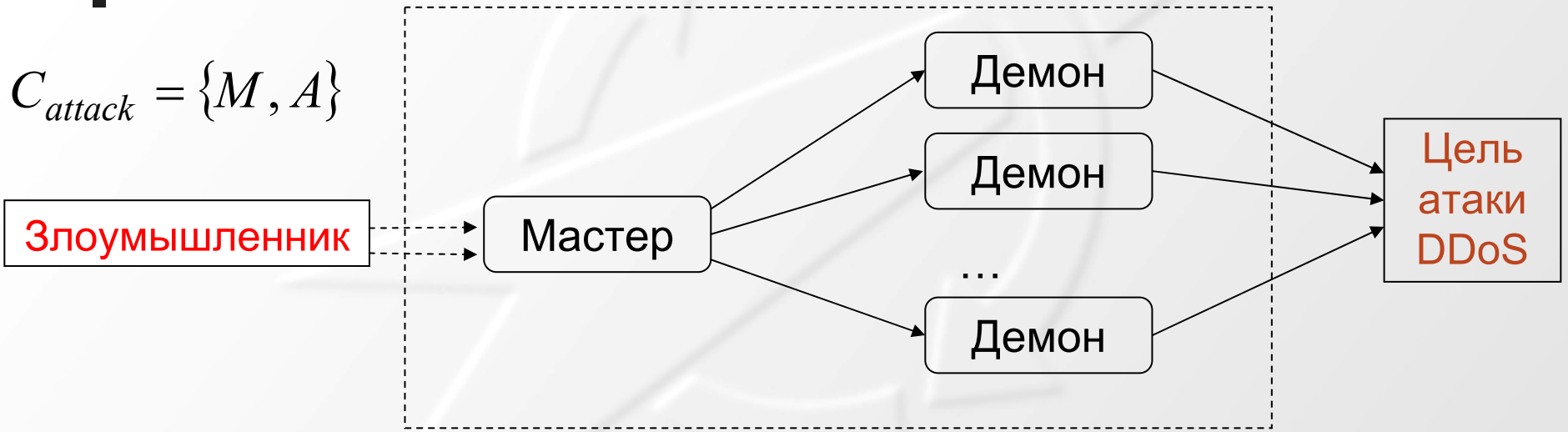
- Предлагаемый подход базируется на **комбинировании** элементов теории общих намерений, теории разделяемых планов и комбинированных подходов
- **Структура команды агентов** описывается в терминах иерархии групповых и индивидуальных ролей в различных сценариях действий
- **Спецификация иерархии планов** действий осуществляется для каждой из ролей. Для каждого плана описываются:
  (1) начальные условия, когда план предлагается для исполнения;
  (2) условия, при которых план прекращает исполняться;
  (3) действия, выполняемые на уровне команды, как часть общего плана
- **Назначение ролей и распределение планов** между агентами выполняется в два этапа: (1) сначала план распределяется в терминах ролей, (2) каждой из ролей ставится в соответствие агент

Процедуры поддержки командной работы

1. **Процедуры обеспечения согласованности действий агентов в команде** *(группе, индивидуально)* по некоторому общему плану.
2. **Процедуры мониторинга и восстановления функциональности команды** *(группы, индивидуально)* за счет переназначения “утерянных” ролей тем членам команды, которые в состоянии выполнить эту работу
3. **Процедуры обеспечения селективности коммуникаций**; основываются на расчете важности того или иного сообщения с учетом его “стоимости” и выгоды, получаемой при этом.

Команда атаки

$$C_{attack} = \{M, A\}$$



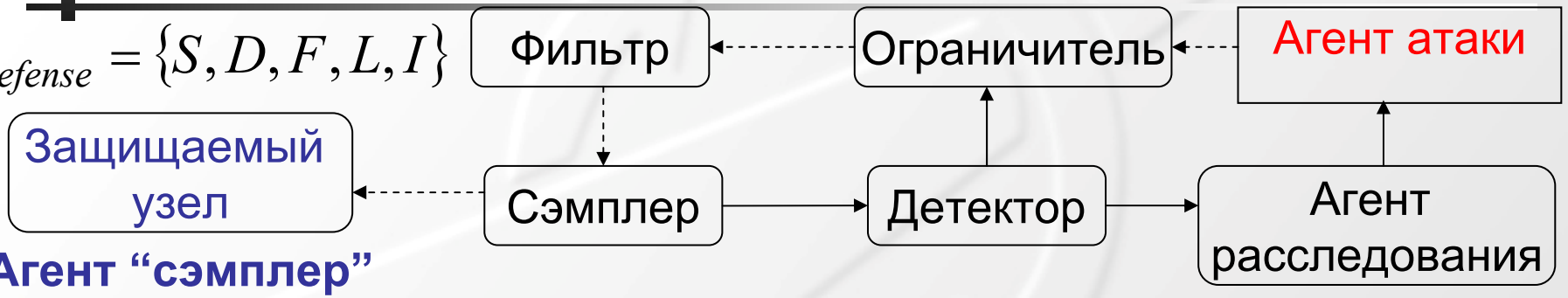
- Атака DDoS: глобальная цель достигается скоординированными усилиями многих компонентов
- «Демон» – исполнитель атаки
  - В начале работы посылает «мастеру» свой адрес и порт
- «Мастер» – координатор атаки
  - Составляет список работоспособных «демонов»
  - Получает команду атаки от злоумышленника
  - Посылает работоспособным «демонам» команду атаки: IP адрес и порт цели, интенсивность (пакетов в секунду)

Параметры моделирования атак (1)

Параметры моделирования атак (2)

Команда защиты

$C_{defense} = \{S, D, F, L, I\}$



Агент “сэмплер”

- Сбор модельных данных для каждого узла по сетевым пакетам
- Выдача модельных данных на запрос «детектора»

Агент “детектор”

- Прием сообщения о работоспособности других агентов
- Запрос данных от «сэмплеров»
- Прием решения об атаке
- Посылка сообщения со списком подозрительных узлов «фильтру» и агенту «расследования», директиву ограничивать трафик

Агент «фильтр» – прием данных от «детектора» и фильтрация

Агент «расследования» – отслеживание источника атаки и его обезвреживание

Агент «ограничитель» – ограничение трафика

Параметры моделирования защиты (1)

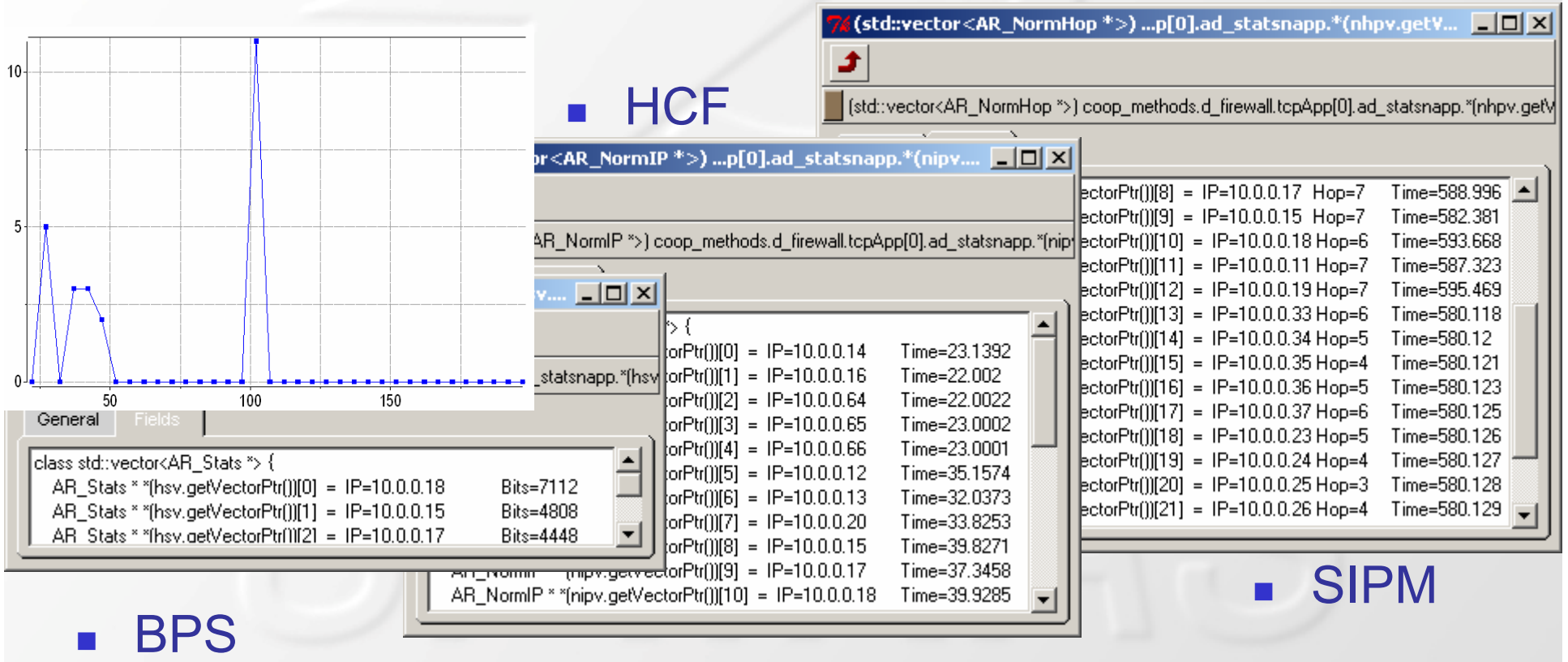
Параметры моделирования защиты (2)

Примеры методов обнаружения вредоносного трафика

- **Hop counts Filtering (HCF):** заключается в формировании таблиц подсетей и количества скачков до них. Предполагается, что пакеты из одной и той же сети проходят от отправителя до получателя одинаковое количество хопов (скачков). Вначале составляется таблица, в которой узлы группируются по количеству хопов. При обнаружении атаки система, реализующая HCF, вычисляет количество хопов пришедшего пакета и сравнивает его с табличным значением.
- **Source IP address monitoring (SIPM):** используется предположение, что во время атаки появляется большое количество новых адресов клиентов. Вначале производится формирование базы IP-адресов “легитимных” клиентов. В реальном времени система собирает статистику по пакетам – количество новых для системы IP-адресов за заданные отрезки времени. Если эта величина остается в пределах нормы, то новые адреса заносятся в базу, если нет – осуществляется фильтрация.
- **Bit Per Second (BPS):** позволяет обнаружить атакующих по превышению порога нормального трафика. Вначале определяется «допустимый» порог для трафика на основе запросов легитимных клиентов.

Построение модели нормального трафика

- Режим обучения:
  - Легитимные клиенты обращаются к защищаемому серверу, а он обрабатывает их запросы, таким образом создавая выборку нормального трафика.
  - Аналогичным образом создается выборка вредоносного трафика, при этом задействуются атакующие агенты команды атаки.

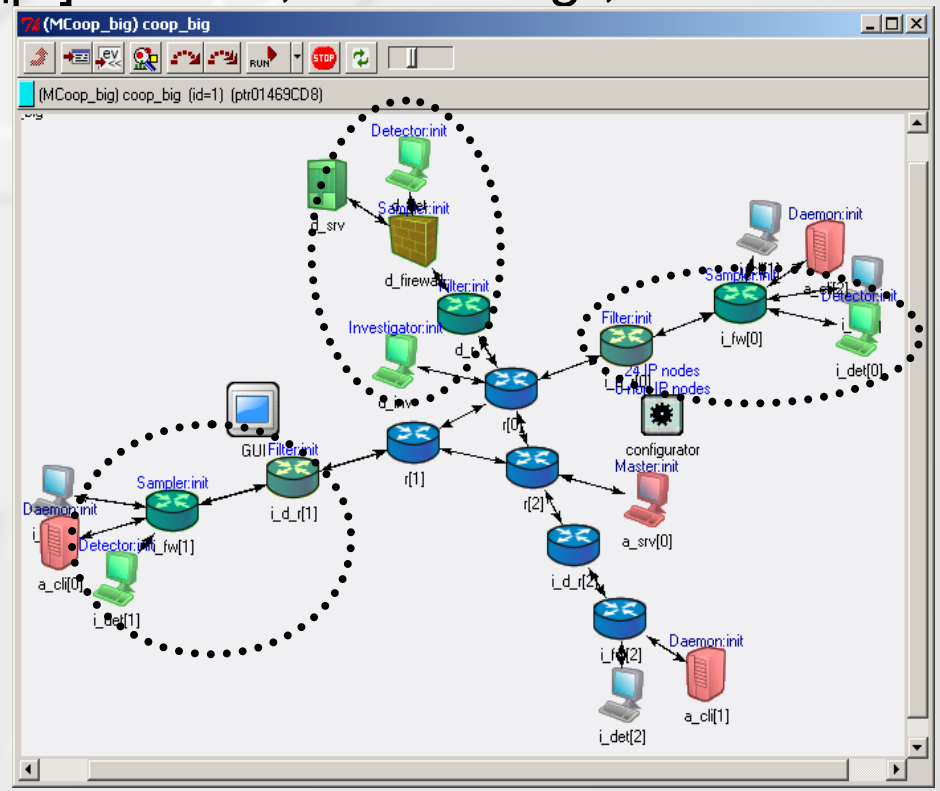


Кооперативные механизмы защиты

- **Модели кооперативного взаимодействия**:
  - DefCOM [Миркович и др.]: “Alert generator”, “Rate limiter”, “Classifier”
  - COSSACK [Пападополус и др.]: “snort”, “watchdog”, filter

Предложенные:

- *без кооперации*;
- *кооперация на уровне фильтров*;
- *кооперация на уровне сэмплеров*;
- *слабая кооперация*;
- *полная кооперация*.

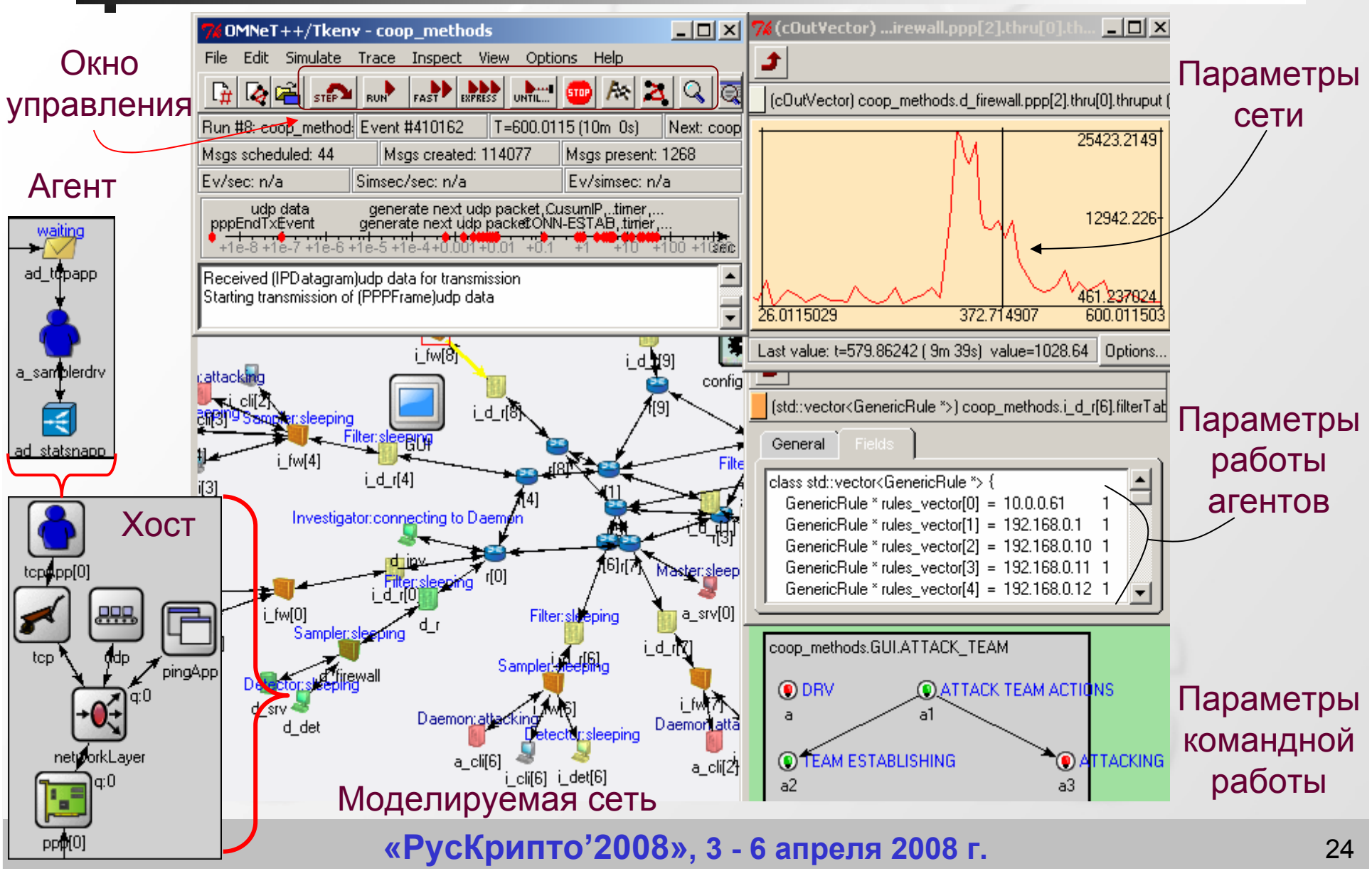


Архитектура среды моделирования

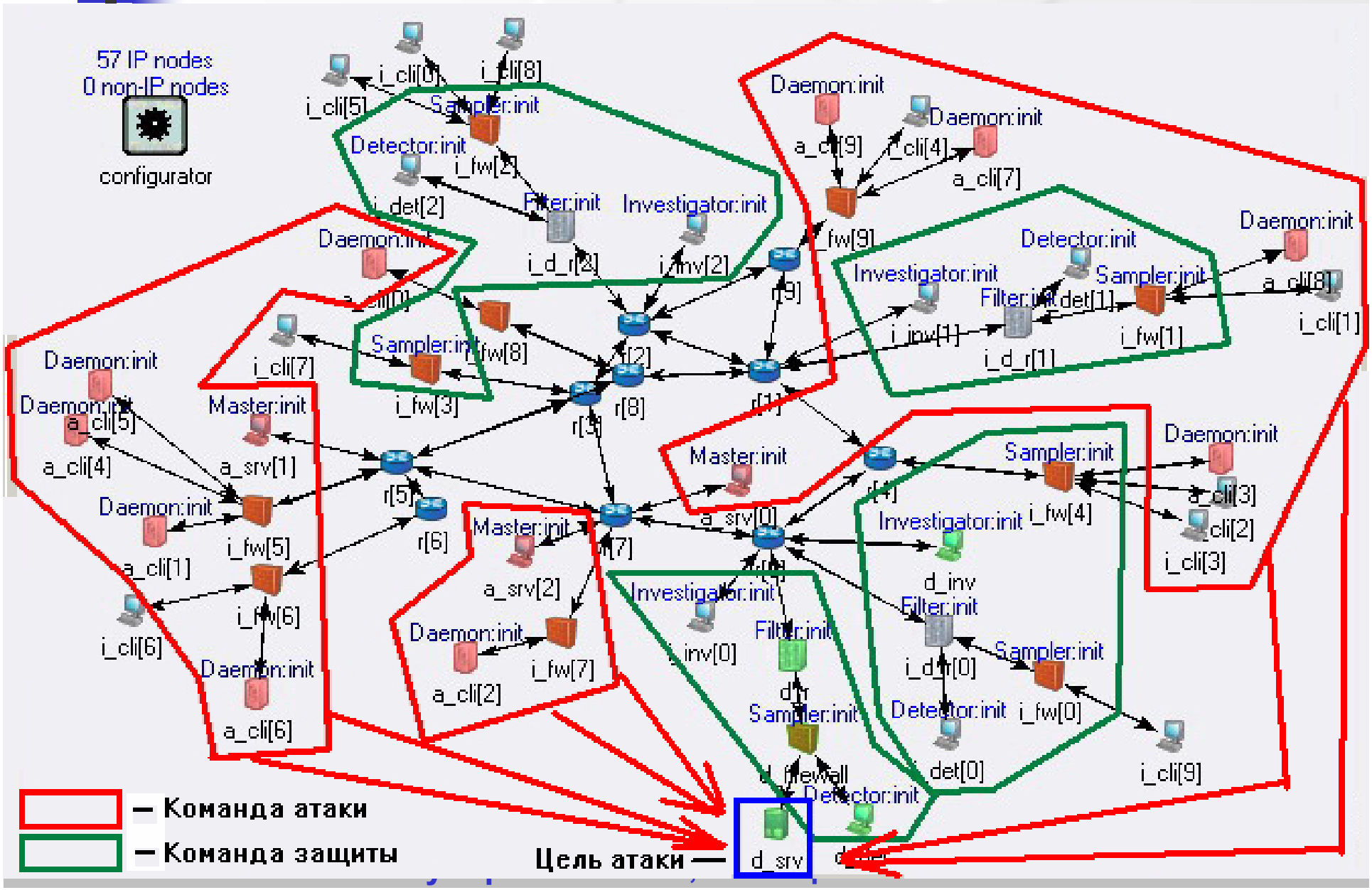
Среда моделирования

- Моделируемые процессы происходят в сети Internet
- Был проведен анализ пакетов моделирования: NS2, OMNeT++ INET Framework, SSF Net, J-Sim INET Framework и др.
- Выдвинутым требованиям удовлетворяет OMNET++ INET Framework (надстройка над OMNET++)
- OMNET++ – симулятор дискретных событий, которые происходят внутри модулей
- Модуль имеет шлюзы, через которые по каналам передаются сообщения
- INET Framework был доработан и дополнен новыми модулями для корректного моделирования механизмов атаки и защиты
- На его основе разрабатывается многоагентная среда моделирования борьбы за ресурсы в сети Internet

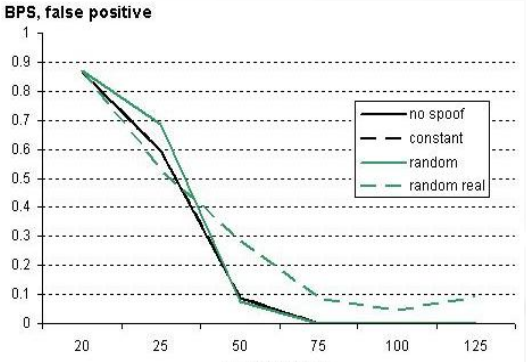
Разработанная среда

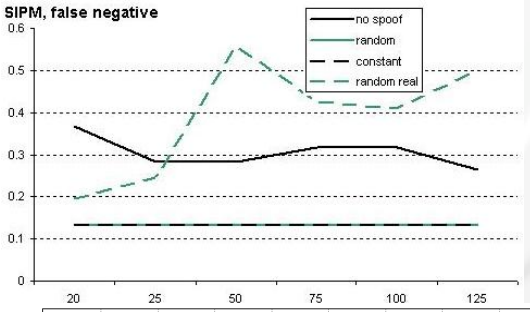


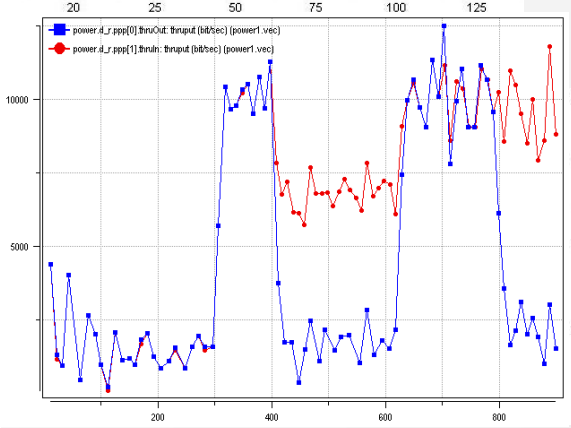
Пример моделируемой сети



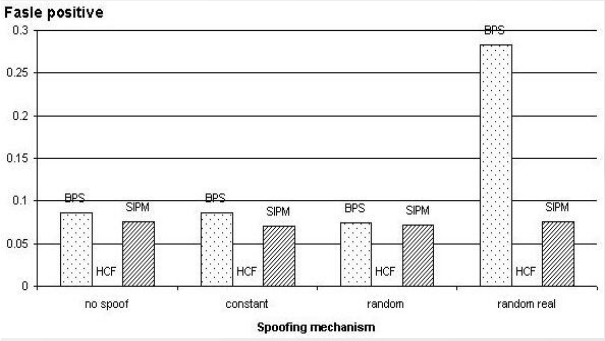
Эксперименты

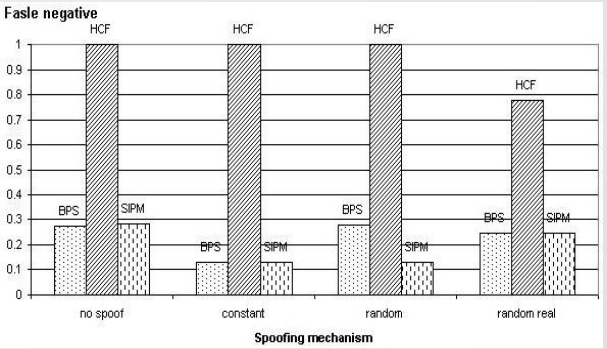






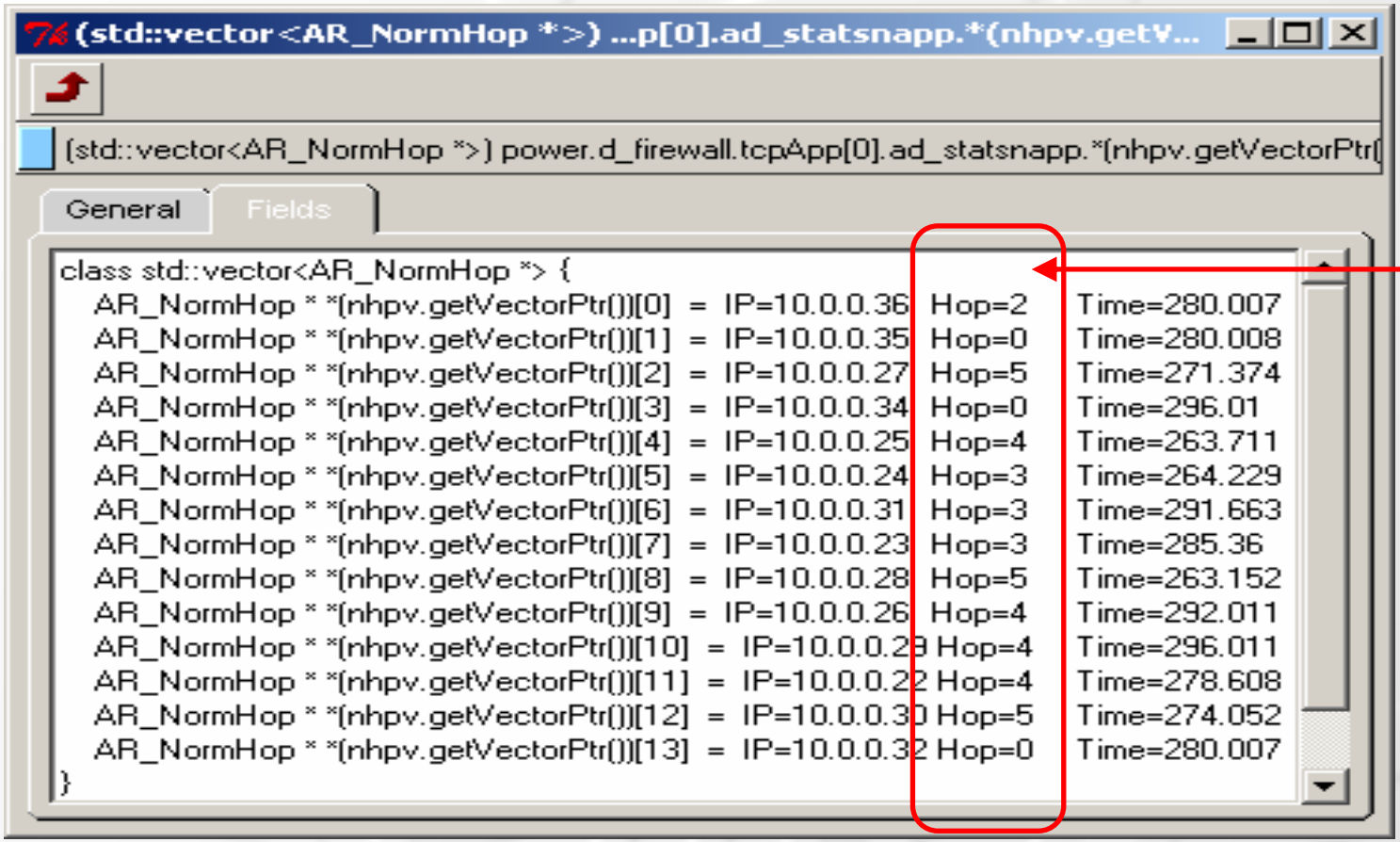
- Созданная среда моделирования позволяет проводить различные эксперименты с целью исследования стратегий реализации атак и перспективных методов защиты.
- В процессе экспериментов можно варьировать
  - топологию и конфигурацию сети;
  - структуру и конфигурацию команд атаки и защиты;
  - механизмы реализации атак и защиты;
  - параметры кооперации команд и др.





Режим обучения (1)

для Hop counts Filtering (HCF)



Коли-
чество
скачков

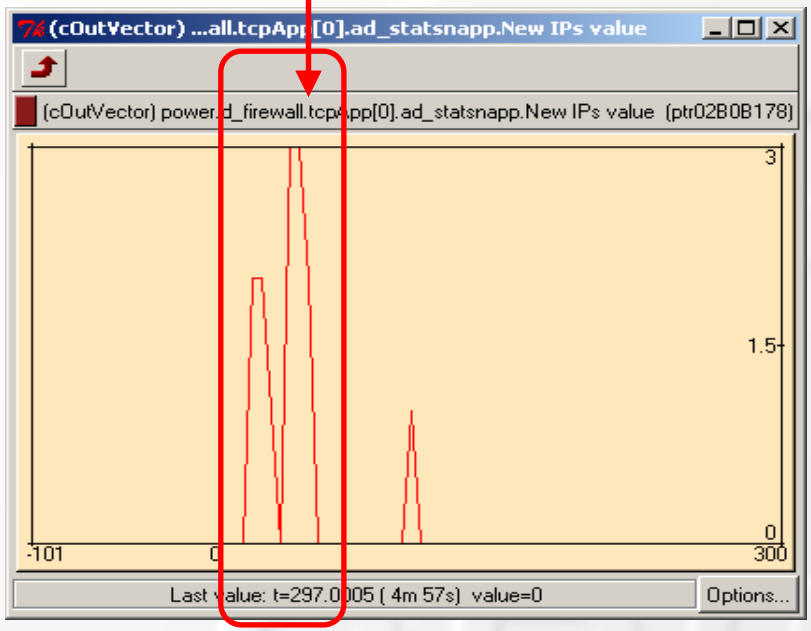
Список узлов, обращавшихся к серверу, и скачков до них после 300 секунд обучения

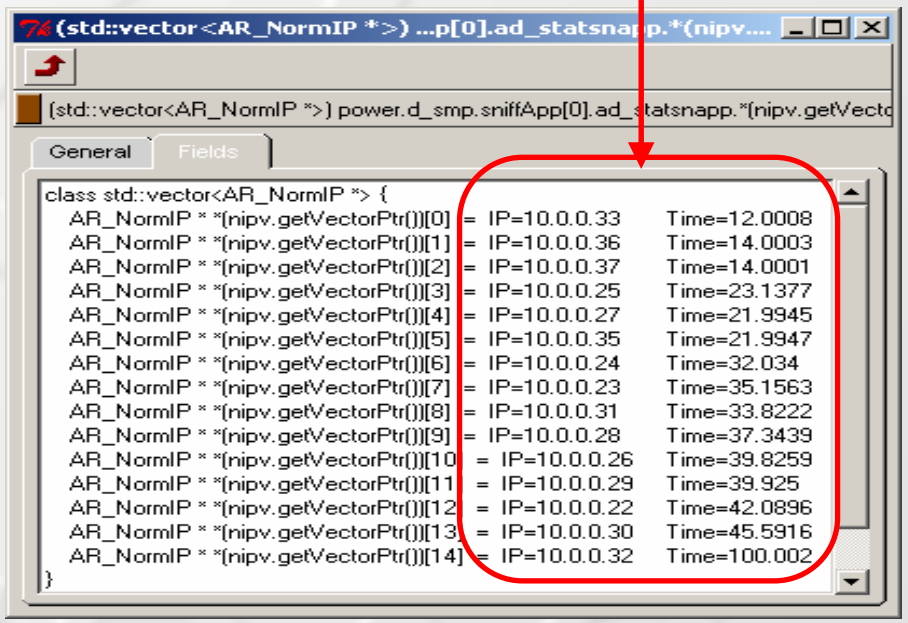
Режим обучения (2)

для Source IP address monitoring (SIPM)

Много новых адресов в начале

Много новых адресов в интервале между 0 и 50 сек





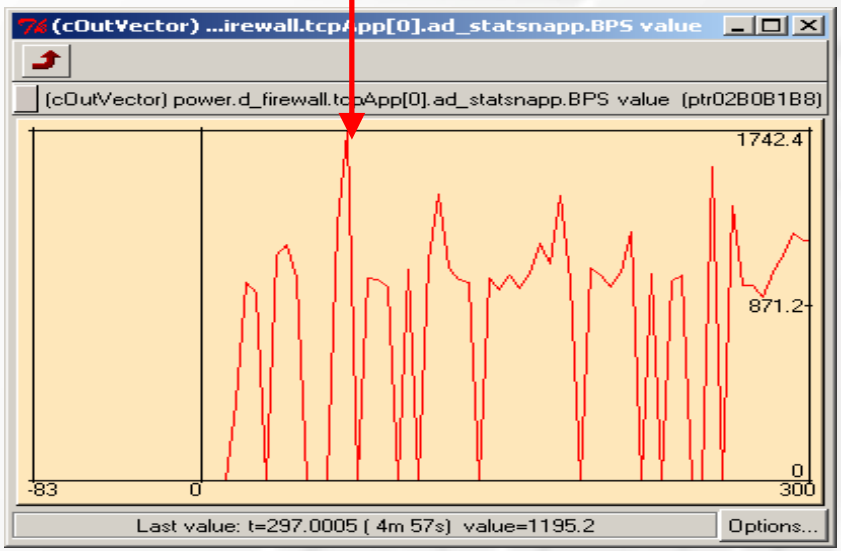
Изменение количества новых IP-адресов

Список узлов, обращавшихся к серверу и признанных легитимными клиентами после 300 секунд обучения

Режим обучения (3)

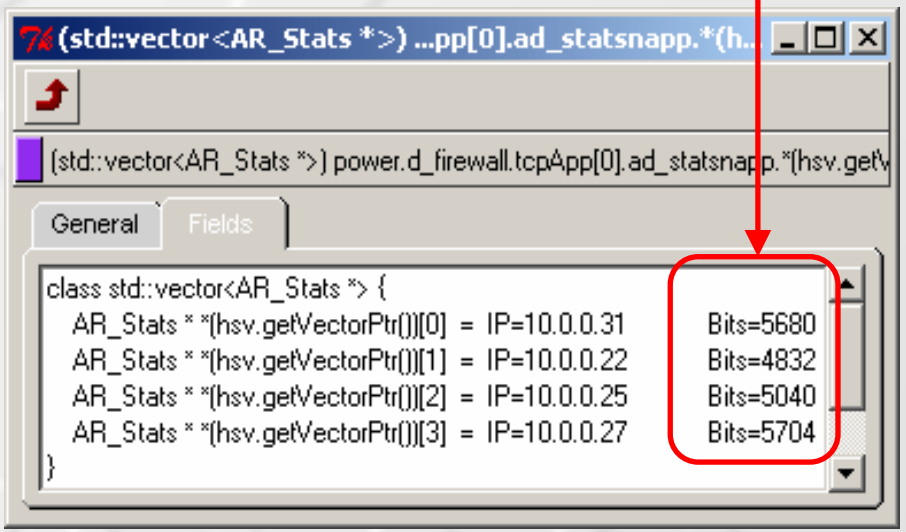
для Bit Per Second (BPS)

Максимальное значение - 1742.4 бит/сек



Изменение параметра BPS

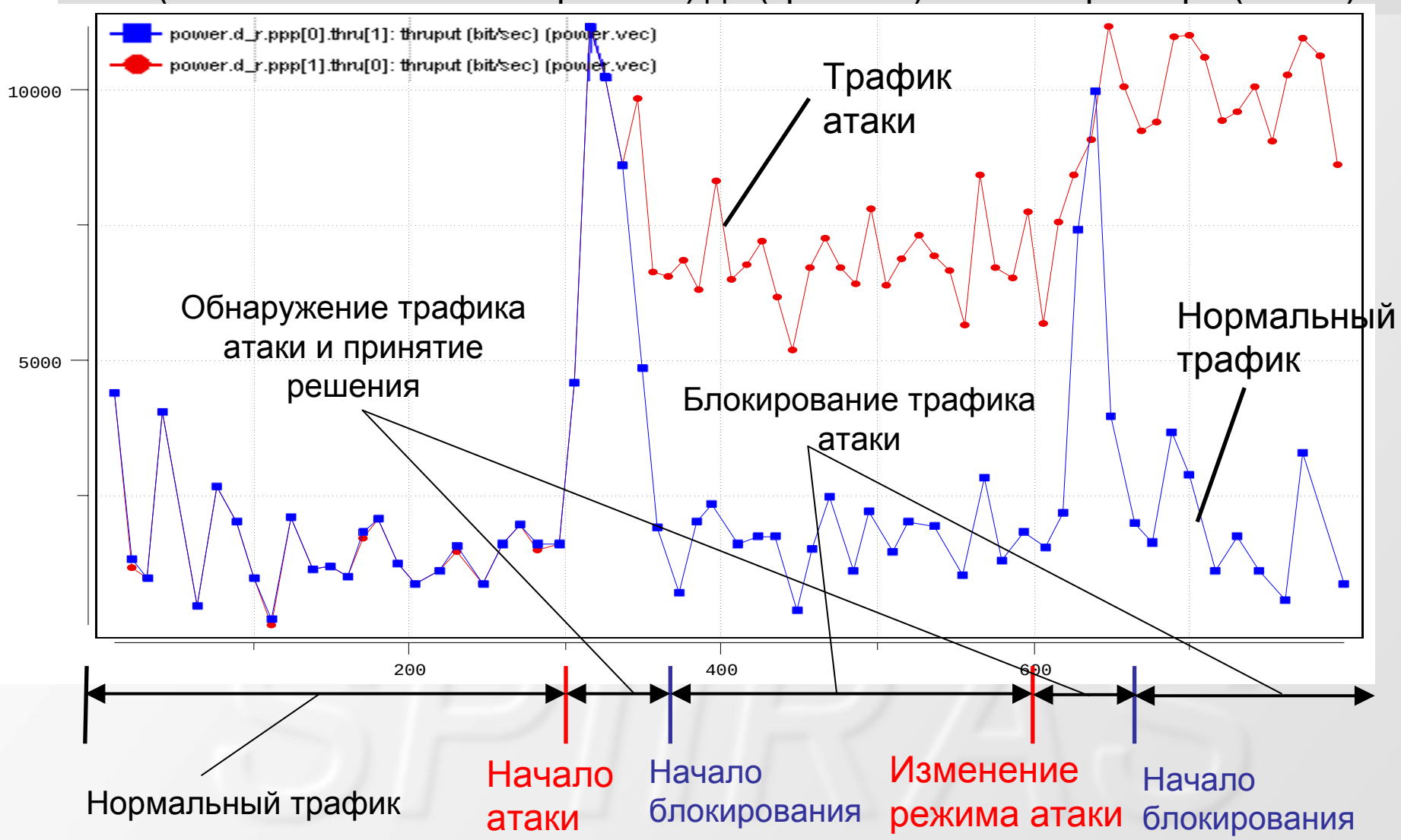
Количество бит в интервале 10 сек



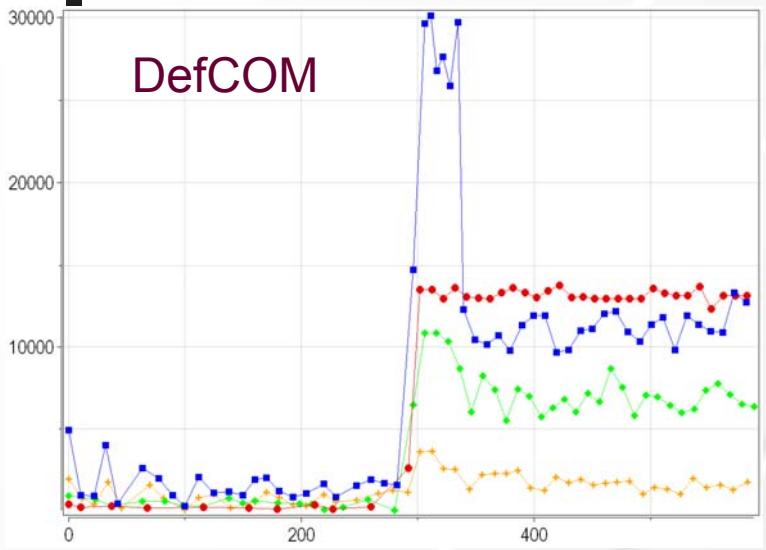
Статистика количества переданных бит по одному из интервалов времени

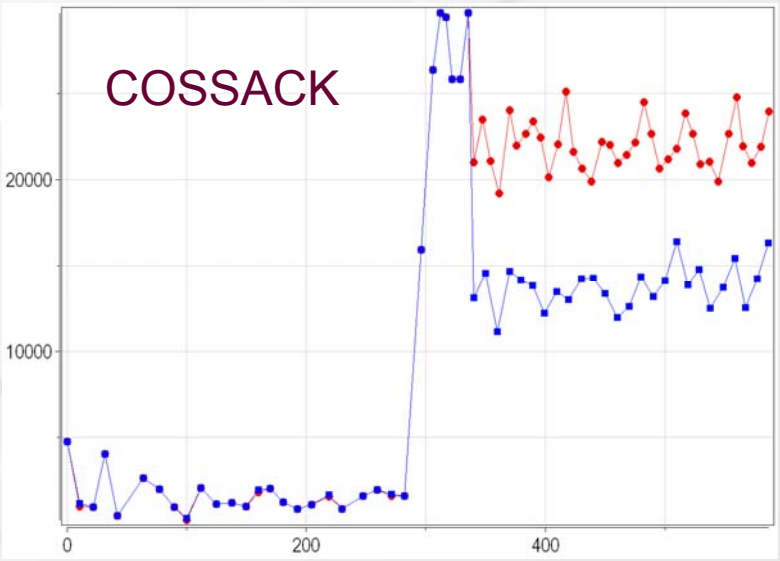
Принятие решения и функционирование

Графики изменения пропускной способности канала на входе в защищаемую сеть (зависимость бит/с от времени) до (красный) и после фильтра (синий)



Графики трафика для механизмов кооперации





- Параметры: топология опорной сети: k=2, количество узлов – 10, параметр *z* = 2.25, 10 клиентов подключены случайным образом к маршрутизаторам опорной сети, задан защищаемый сервер и параметры осуществления запросов к нему клиентов. В команду атаки входят 10 демонов, реализующих атаку UDP flood на сервер.

Основные результаты работы

- Разработана программная среда моделирования механизмов защиты от DDoS атак
- С использованием разработанной среды проведено множество экспериментов
- Исследовались различные типы атак, оптимальные параметров механизмов защиты
- Проведено сравнение различных механизмов защиты, режимов кооперации
- В дальнейшем планируется совершенствование среды моделирования, расширение библиотеки предметной области и системы многоагентного моделирования.

Контактная информация

Котенко Игорь Витальевич (СПИИРАН)
ivkote@iias.spb.su
http://comsec.spb.ru/kotenko/

Благодарности

Работа выполнена при финансовой поддержке РФФИ (проект №07-01-00547), программы фундаментальных исследований ОИТВС РАН (контракт №3.2/03), Фонда содействия отечественной науке и при частичной финансовой поддержке, осуществляемой в рамках проектов Евросоюза POSITIF (контракт IST-2002-002314) и RE-TRUST (контракт № 021186-2).

РОССИЙСКАЯ АКАДЕМИЯ НАУК