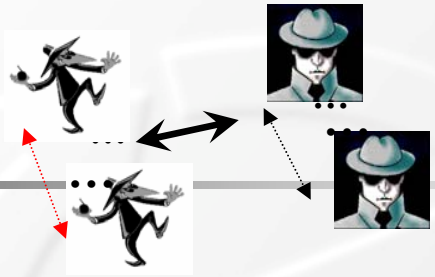
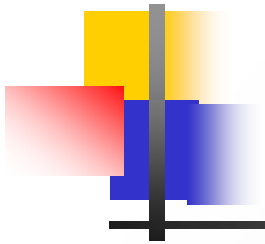


“СЕТЕВЫЕ КОШКИ-МЫШКИ”: ВОЙНЫ АДАПТИВНЫХ ПРОГРАММНЫХ АГЕНТОВ

И.В. Котенко

Санкт-Петербургский институт информатики и автоматизации РАН

РусКрипто’2009, 2-5 апреля 2009 г.



План доклада

- Введение
- Подход к моделированию
- Механизмы адаптации
- Среда моделирования
- Эксперименты
- Заключение

Важность и актуальность проблемы (1/2)

- В настоящее время мы являемся свидетелями новой фазы противостояния (“гонки вооружений”) в открытых сетях между средствами нападения и защиты
- Традиционно атакующие имеют некоторое преимущество перед защищающимися
- Текущее состояние противодействия систем нападения злоумышленников и систем защиты хакеры характеризуют как “игру в сетевые кошки-мышки” (a game of Network Cat and Mouse) – кто кого обманет [Nomad Mobile Research Centre]

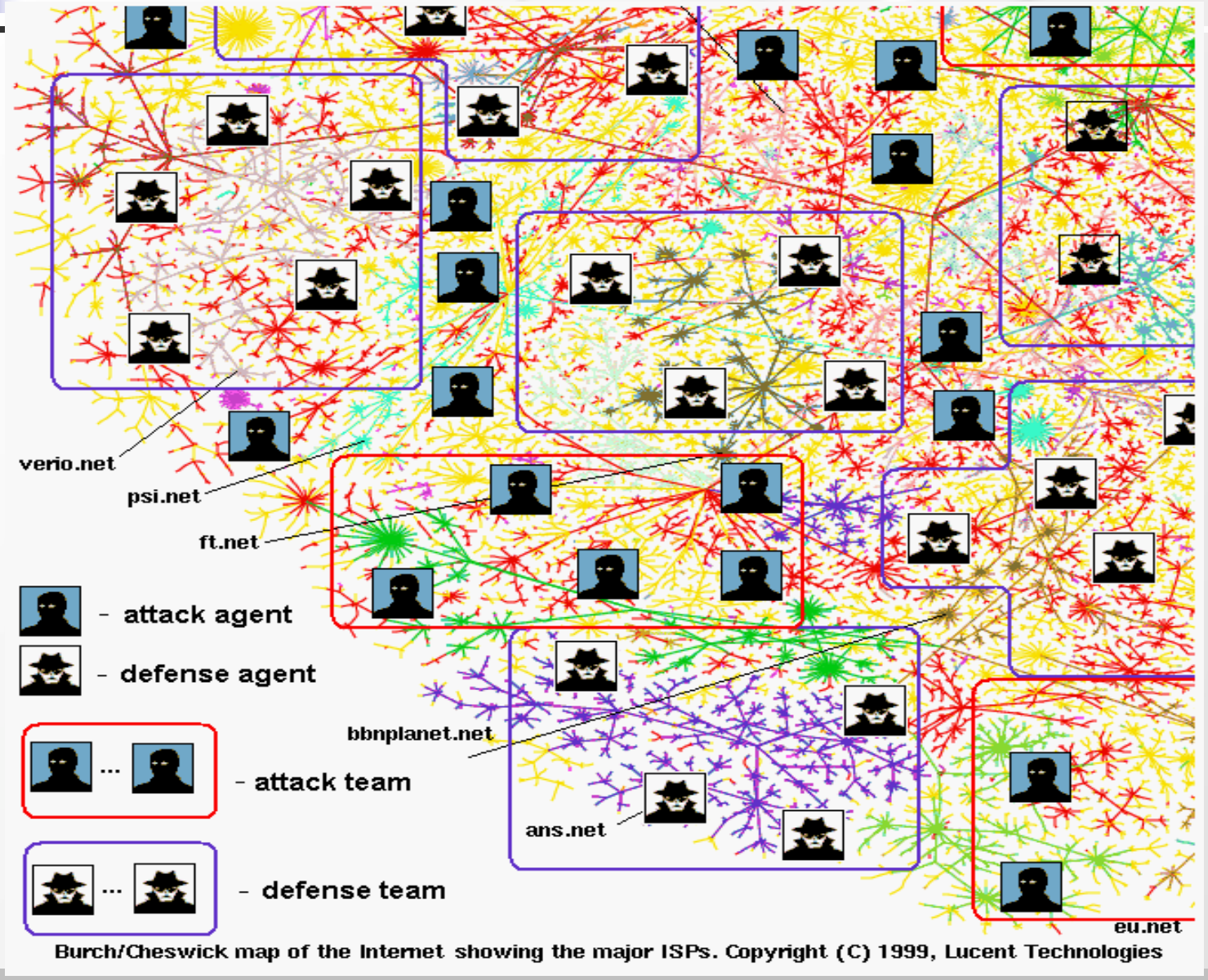
Важность и актуальность проблемы (2/2)

- Современные системы защиты в Интернет должны динамически изменяться при изменении как самой защищаемой целевой системы, так и с изменением среды функционирования
- Для реализации этих возможностей в перспективных системах защиты необходимо обеспечить динамическое поведение, автономность и адаптацию отдельных компонентов, использовать методы, основанные на переговорах и кооперации, которые лежат в основе многоагентных систем и (или) автономных вычислений
- Моделирование и имитационные эксперименты стали необходимым фундаментом для исследований в области компьютерных наук, включая область компьютерной и сетевой безопасности

Цель и задачи работы

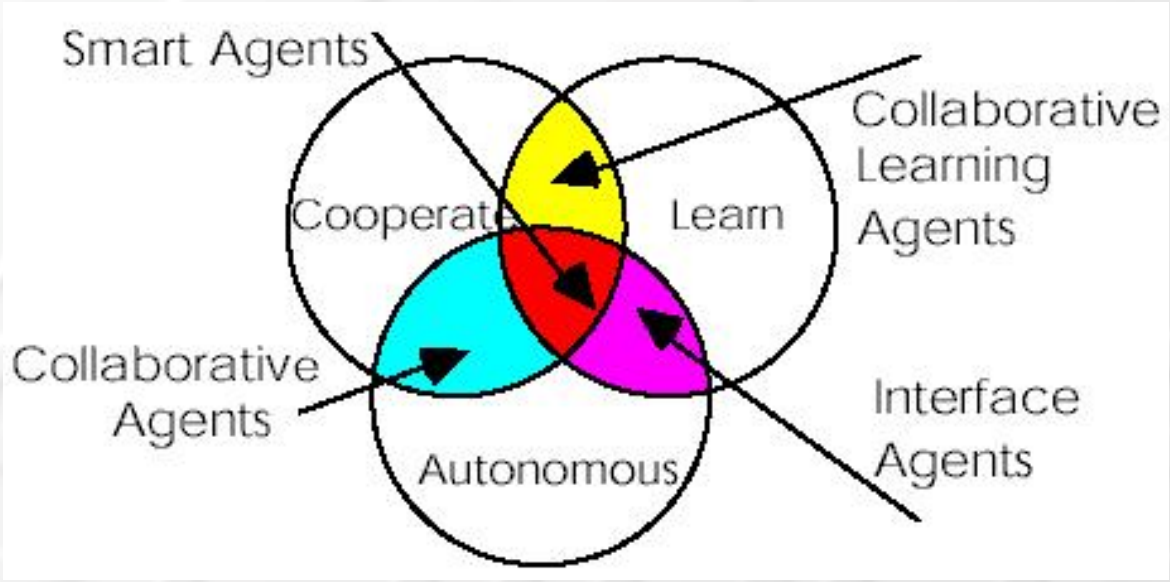
- **Цель работы:** *исследование возможности применения предлагаемого агентно-ориентированного подхода и разработанной среды моделирования для* ***исследования адаптивного поведения противоборствующих команд интеллектуальных агентов*** *на примере механизмов защиты* от *атак “Распределенный отказ в обслуживании” (Distributed Denial of Service, DDoS).*
- *Эволюционный подход к разработке подхода*
- В отличие от предыдущих работ авторов наибольший акцент делается на исследовании **адаптивных сценариев** противодействия команд агентов атаки и защиты и описании проведенных экспериментов

Подход к моделированию

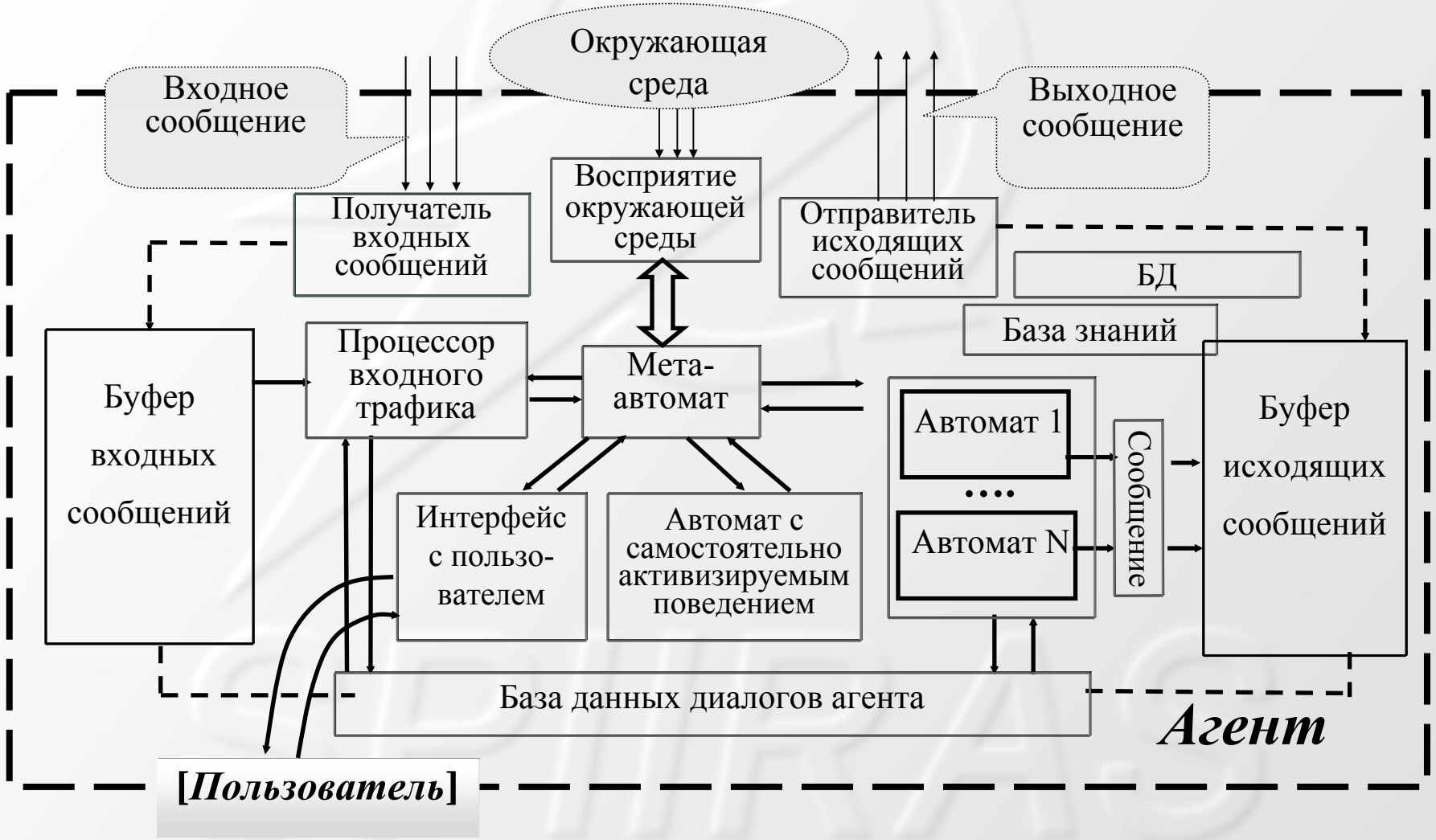


Интеллектуальные агенты

Интеллектуальные программные агенты – программные компоненты, которые могут выполнять специфические задачи, поставленные пользователем, и обеспечивать такую степень интеллекта, которая позволяет выполнять эти задачи автономно, адаптируясь к среде и взаимодействуя со средой и другими агентами рациональным способом.



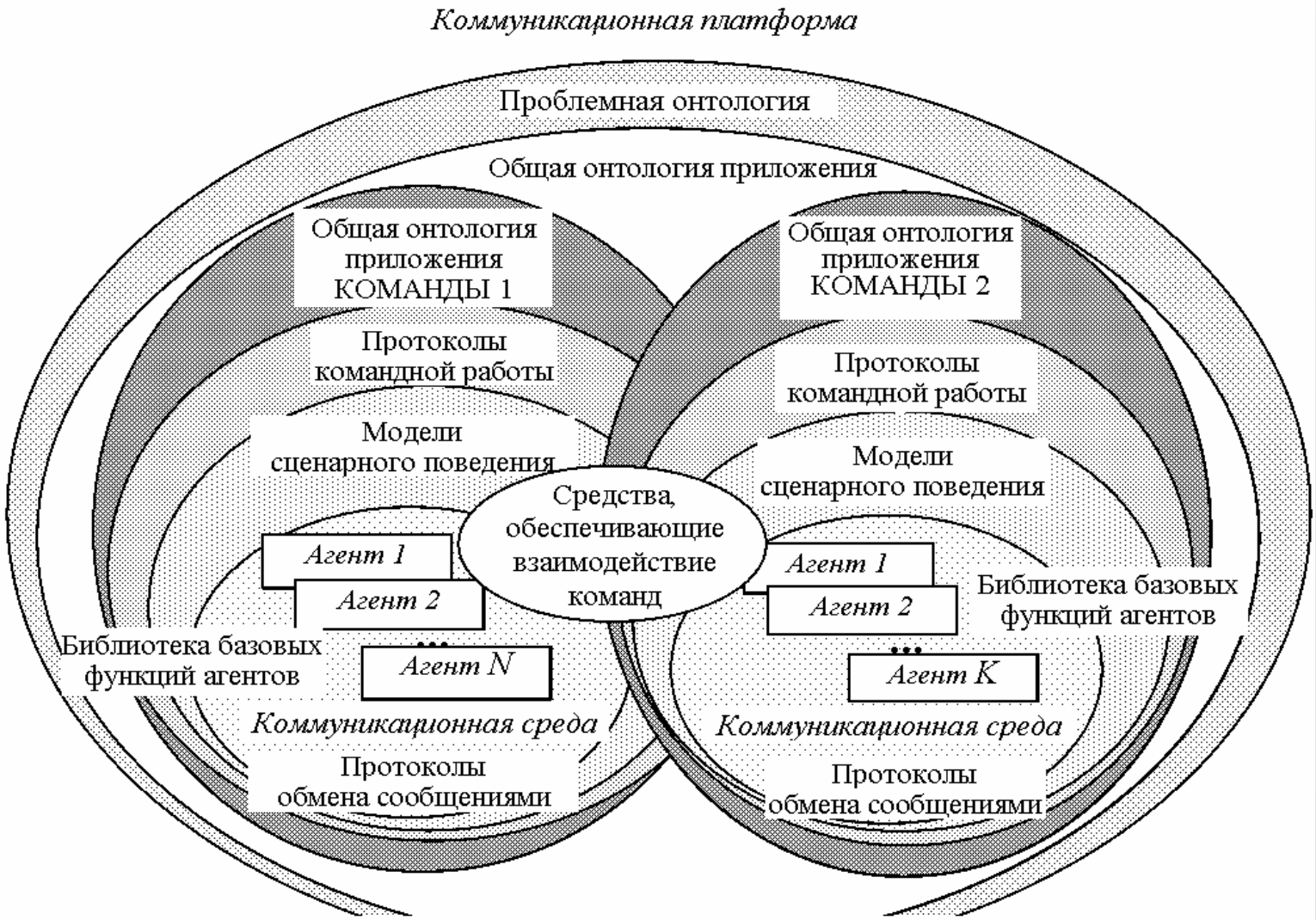
Стандартная архитектура агента



Подход к моделированию

- Кибернетическое противоборство представляется в виде взаимодействия различных команд программных агентов
- Процессы происходят в среде, задаваемой моделью Интернета
- Выделяются команды агентов атаки, защиты и пользователей
- Команды взаимодействуют между собой: противоборствуют, кооперируются, адаптируются
- Команда агентов-злоумышленников эволюционирует посредством генерации новых экземпляров и типов атак, а также сценариев их реализации с целью преодоления подсистемы защиты.
- Команда агентов защиты адаптируется к действиям злоумышленников путем изменения исполняемой политики безопасности, формирования новых экземпляров механизмов и профилей защиты.

Модель взаимодействия команд агентов



Модели среды функционирования: топологический и функциональный компоненты

Особенности защиты от атак DDoS

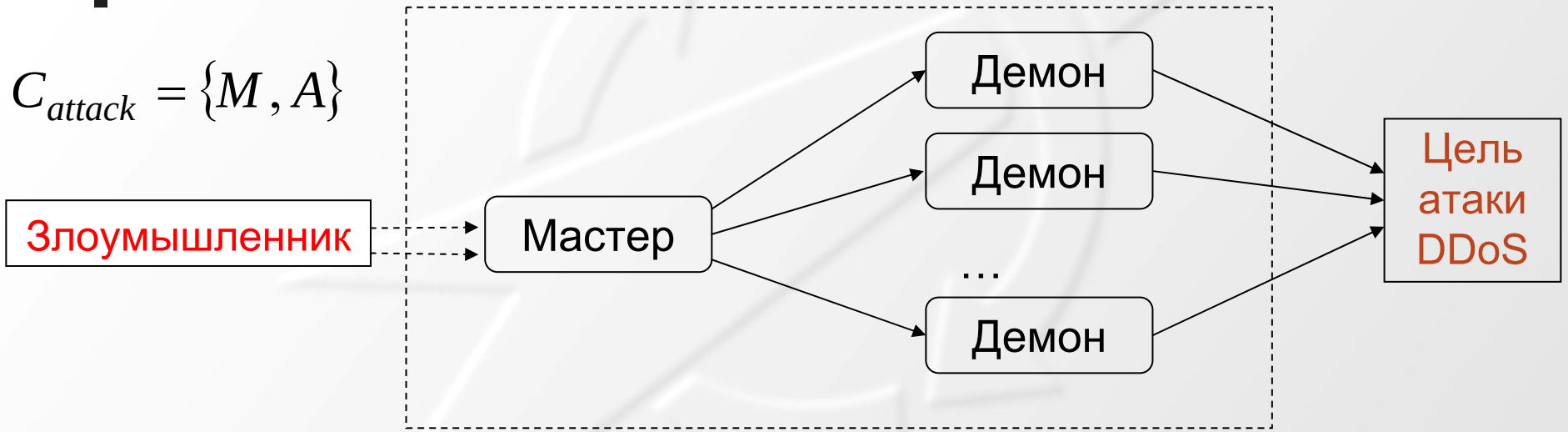
- Назначение: быстро определять и реагировать на атаки [Xiang, Zhou, 04], доставлять легитимный трафик [Mirkovic, et al., 05].
- Различные характеристики сети используются для обнаружения атак (например, IP-адреса атакующих [Peng , et al., 05], уровень трафика [Gil, Poletto, 03], содержимое пакета [Papadopoulos, 03]).
- Чтобы определить аномалии, используются различные методы (например, статистические [Li, et al., 05], сопоставление с образцом…).
- Механизмы реагирования: фильтрация пакетов [Park, Lee, 01], контроль перегрузок [Mahajan, et al., 02], отслеживание [Kuznetsov, et al., 02].
- Общий подход к защите от атак DDoS:
  - 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 (изменение и перенос)**
  - 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

Команда атаки

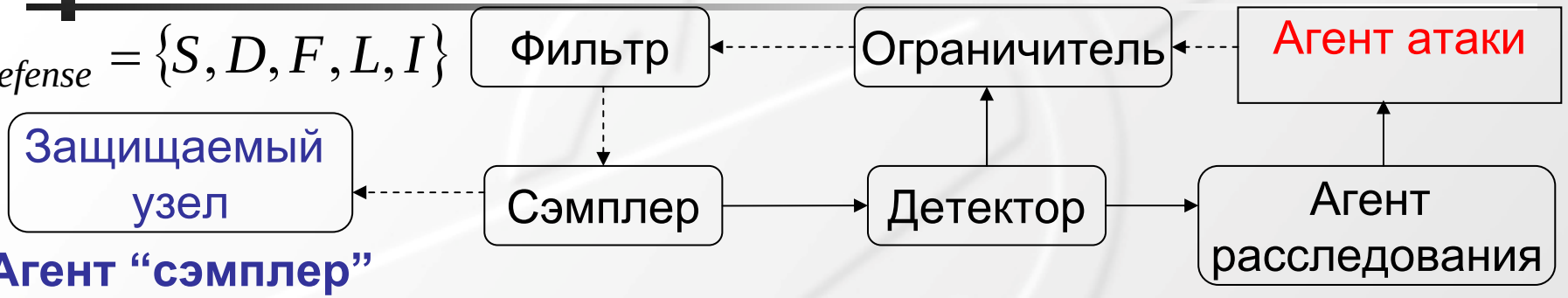
$$C_{attack} = \{M, A\}$$



- 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)

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 исследуемых моделей сети, механизмов защиты и атаки (1/2)

- *Топология сети:* количество и типы хостов и каналов связи между ними.
- *Конфигурация команд атаки:* количество демонов; адрес и порт мастера для взаимодействия; порт демона для посылки пакетов атаки; адрес и порт цели атаки; время атаки; интенсивность атаки; метод подмены адреса отправителя.
- *Параметры реализации атаки*: тип цели атаки (приложение, узел или сеть; необходимо указать IP-адрес и порт цели атаки), тип атаки (грубая сила (UDP/ICMP flood, smurf/fraggle и др.) или семантическая (TCP SYN, Incorrect packets, Hard requests и др.)), темп атаки, схема адаптации и т.п.

Параметры исследуемых моделей сети, механизмов защиты и атаки (2/2)

- *Параметры команды защиты*: адрес защищаемого узла, адрес и порт “детектора” для взаимодействий, размер ответа на запрос и время обработки запроса сервером; схема адаптации и т.п.
- *Параметры механизмов защиты*: расположение, этапы защиты, способ обнаружения и т.п.
- *Параметры команды пользователей*: количество пользователей; адрес и порт сервера; время начала работы; количество, запросов, интервал между запросами, размер запросов к серверу в одном соединении; интервал между соединениями.
- *Параметры кооперации агентов защиты:* схема кооперации.
- *Параметры моделирования*: продолжительность моделирования, количество экспериментов и др.

Критерии адаптации команд агентов (1/2)

- Субъекты взаимодействия (*S*): команды атаки и защиты.
- Общий подход к адаптации:

$$\min_{S(t)} \sum_{i=1}^{n} C_i\left(S(t), K_D(t)\right)$$

Отражает стоимости

Конфигурация системы

Показатель мощности атаки/защиты

  - Критерий адаптации команды защиты:

$$\min_{S(t)} \sum_{i=1}^{n} \left\{C_{FP}\left(S(t), K_D(t)\right) + C_{FN}\left(S(t), K_D(t)\right) + C_T\left(S(t), K_D(t)\right)\right\}$$

Процент ложных срабатываний

Процент пропусков атак

Продолжительность атаки

  - Критерий адаптации команды атаки:

$$\min_{E(t)} \sum_{i=1}^{n} \left\{C_P\left(E(t), K_A(t)\right) + C_D\left(S(t), K_A(t)\right)\right\}$$

Количество пакетов

Количество обезвреженных «демонов»

Критерии адаптации команд агентов (2/2)

$K_D(t) = \{M_i, TK_j\}$ – конфигурация системы защиты на время t,

где M_i – метод защиты и его параметры (полученные во время обучения),

TK_j – схема кооперации (без кооперации, на уровне фильтров, сэмплеров и полная)

$K_A(t) = \{I_i, R_j\}$ – параметры атаки на время t,

где I_i – интенсивность атаки (задается злоумышленником),

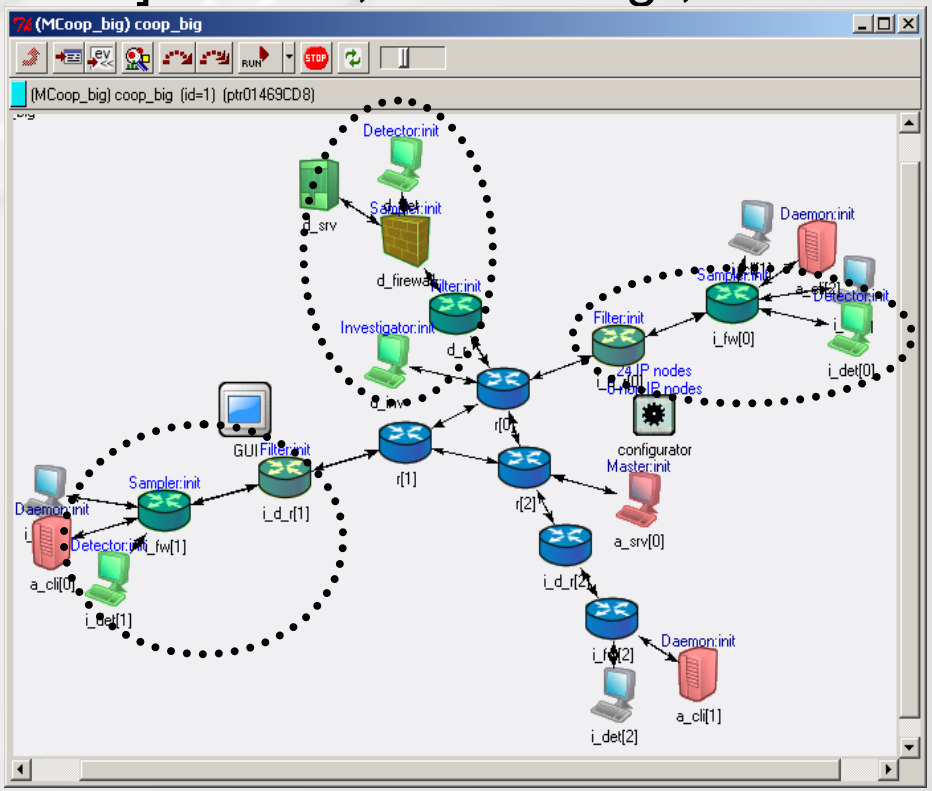
R_j – метод подмены адреса отправителя (без подмены, постоянная, случайная, случайная той же подсети)

Кооперативные механизмы защиты

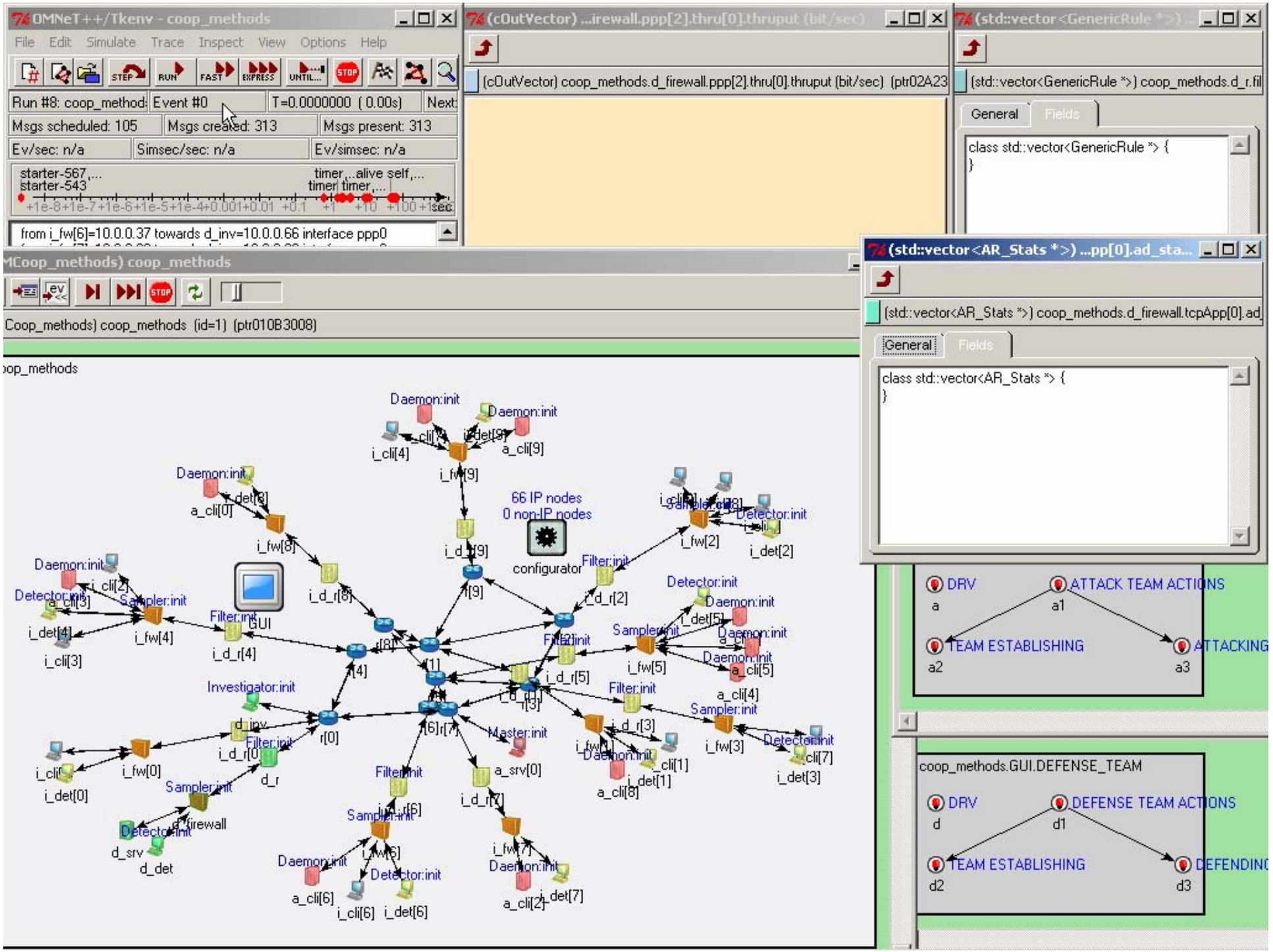
- **Модели кооперативного взаимодействия**:
  - DefCOM [J.Mirkovic, etc., 2005]: “Alert generator”, “Rate limiter”, “Classifier”
  - COSSACK [*C.Papadopoulos,* 2003]: “snort”, “watchdog”, filter

Предложенные:

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



Архитектура среды моделирования

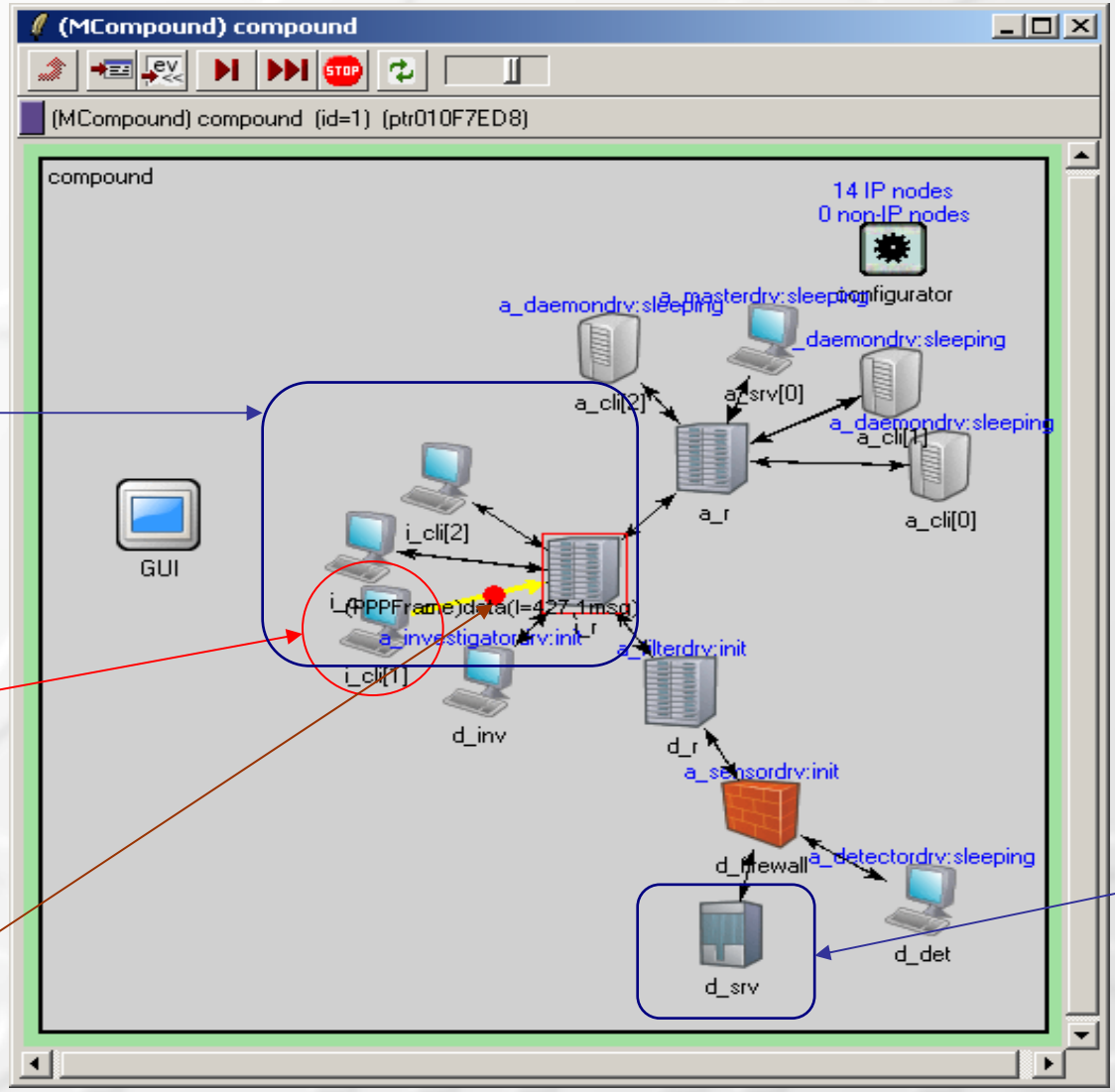

OMNeT++/Tkenv - coop_methods
File Edit Simulate Trace Inspect View Options Help
STEP RUN FAST EXPRESS UNTIL... STOP
Run #8: coop_method: Event #0 T=0.0000000 (0.00s) Next:
Msgs scheduled: 105 Msgs created: 313 Msgs present: 313
Ev/sec: n/a Simsec/sec: n/a Ev/simsec: n/a
starter-567,... starter-543
timer,...alive self,... timer timer,...
+1e-8 +1e-7 +1e-6 +1e-5 +1e-4 +0.001 +0.01 +0.1 +1 +10 +100 +1sec
from i_fw[6]=10.0.0.37 towards d_inv=10.0.0.66 interface ppp0
(cOutVector) ...irewall.ppp[2].thru[0].thruput (bit/sec)
(cOutVector) coop_methods.d_firewall.ppp[2].thru[0].thruput (bit/sec) (ptr02A23
(std::vector<GenericRule *>) coop_methods.d_r.fil
General Fields
class std::vector<GenericRule *> {
}
(std::vector<AR_Stats *>) ...pp[0].ad_sta...
(std::vector<AR_Stats *>) coop_methods.d_firewall.tcpApp[0].ad
General Fields
class std::vector<AR_Stats *> {
}
Coop_methods) coop_methods (id=1) (ptr010B3008)
oop_methods
66 IP nodes
0 non-IP nodes
configurator
GUI
Daemon:init
Sampler:init
Filter:init
Detector:init
Investigator:init
Master:init
DRV
ATTACK TEAM ACTIONS
TEAM ESTABLISHING
ATTACKING
a
a1
a2
a3
coop_methods.GUI.DEFENSE_TEAM
DRV
DEFENSE TEAM ACTIONS
TEAM ESTABLISHING
DEFENDING
d
d1
d2
d3

Фазы противодействия команд агентов: (1) Генерация нормального трафика

Хосты (клиенты), использующие ресурсы Web-сервера d_serv

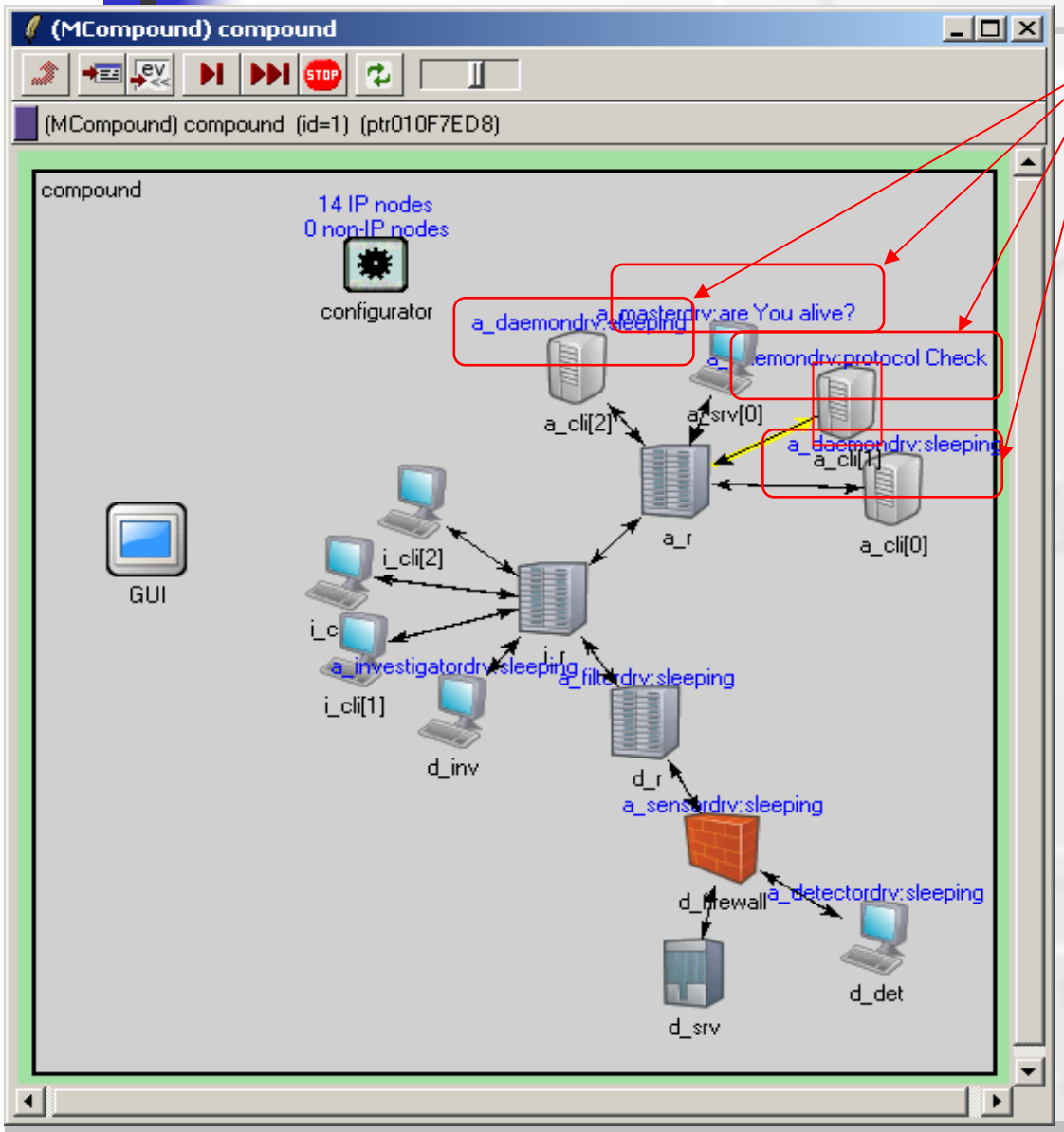
Хост i_cli[1] посылает запрос Web-серверу

Сетевой пакет

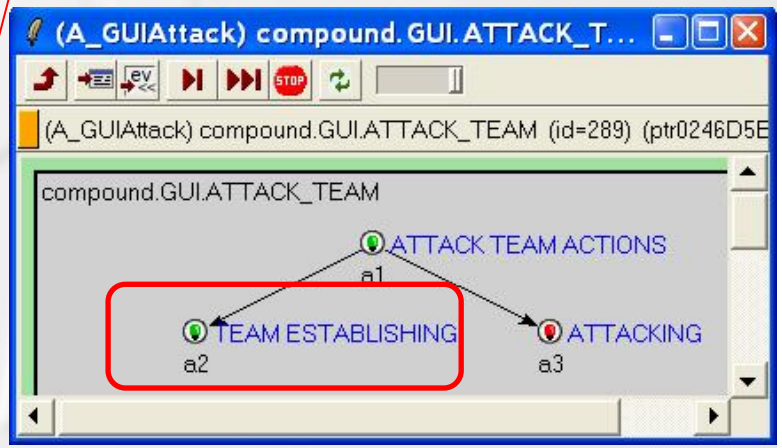


Web-сервер d_serv

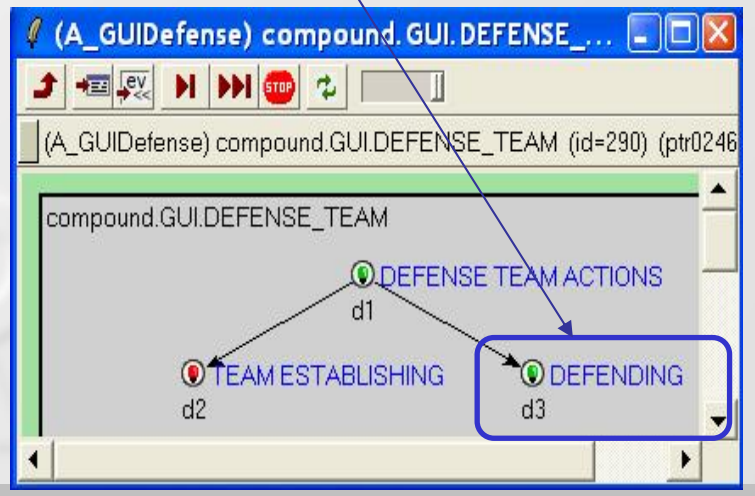
Фазы противодействия команд агентов: (2) Формирование команды атаки



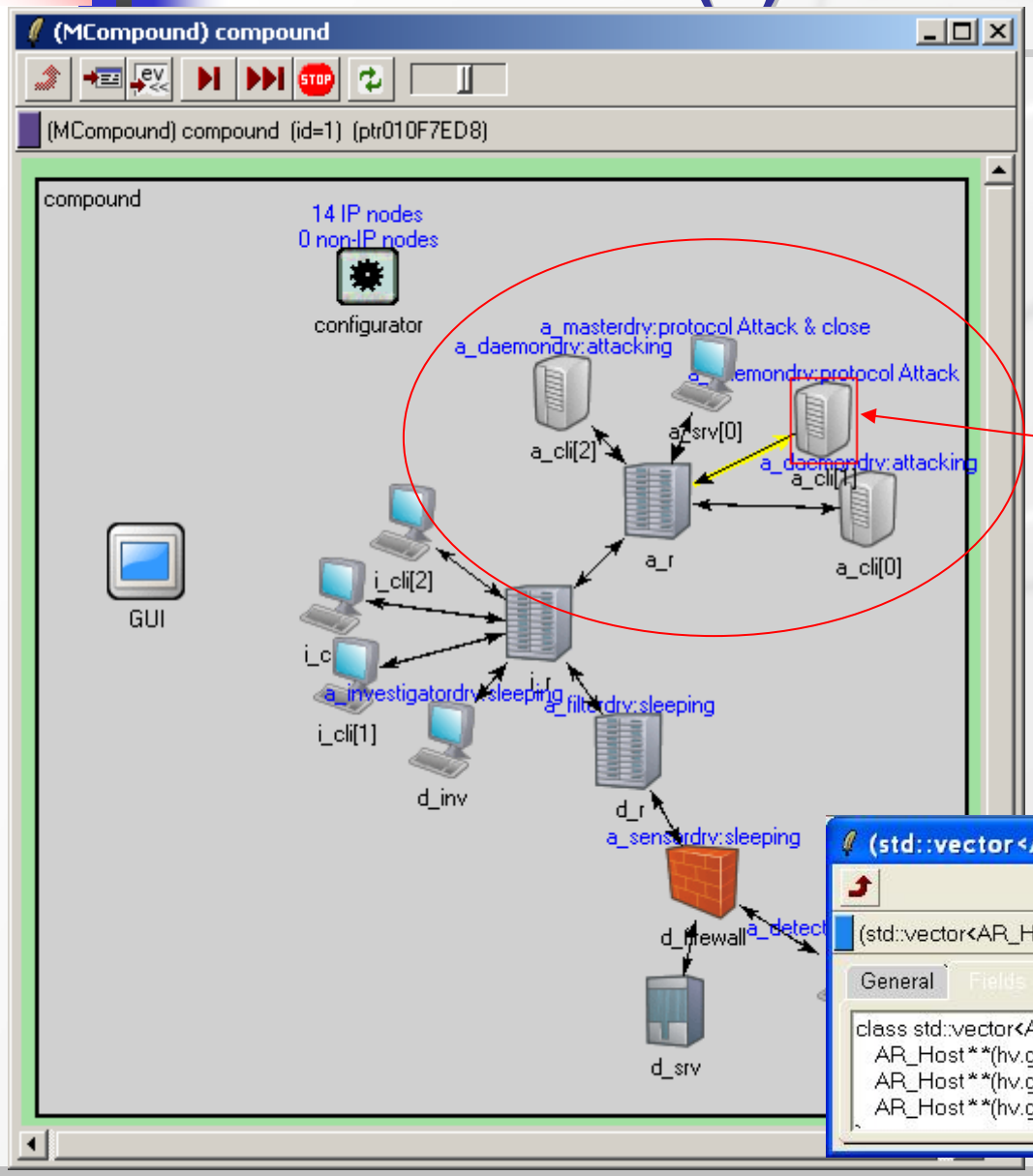
Команда атаки



Команда защиты сформирована



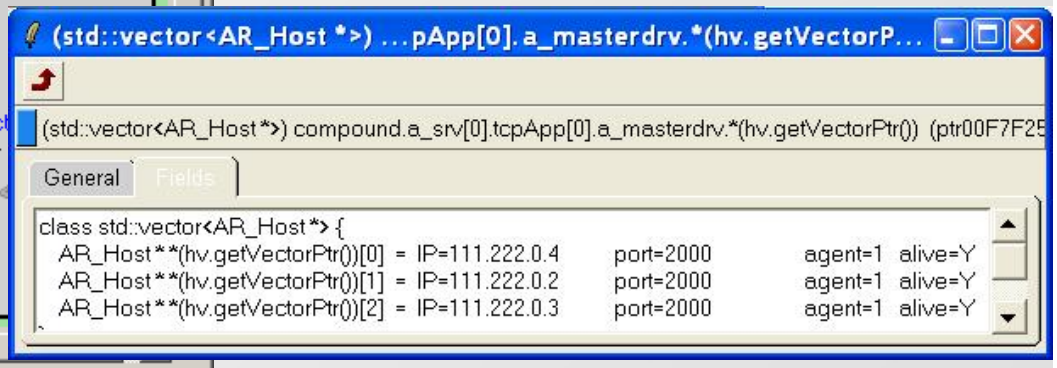
Фазы противодействия команд агентов: (3) Начало атаки



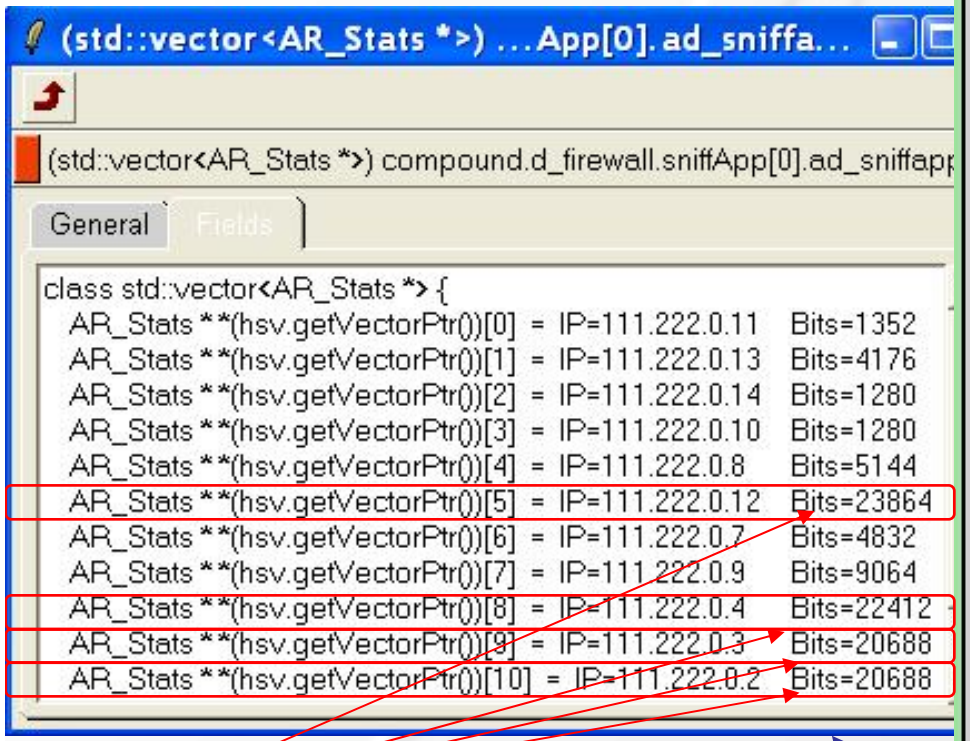
Мастер посылает демонам сообщение об атаке

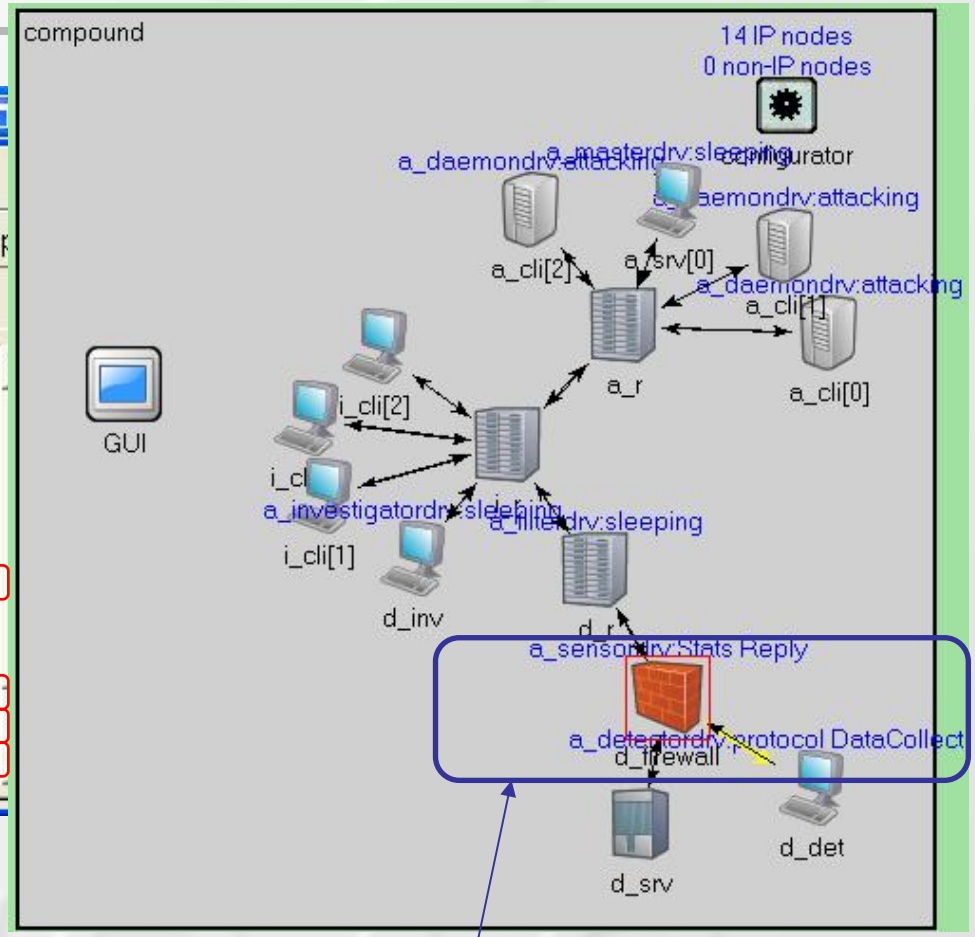
Демоны атакуют

Информация о демонах



Фазы противодействия команд агентов: (4) Действия агента “сэмплер (сенсор)”

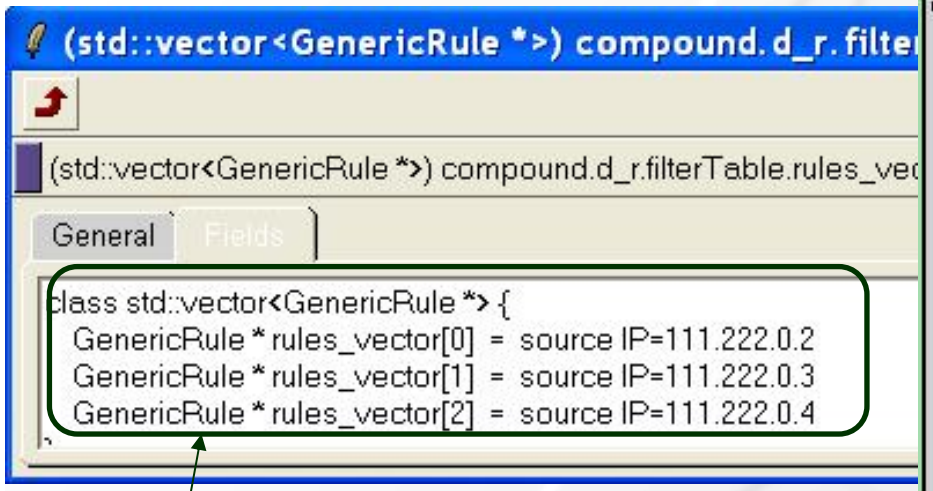


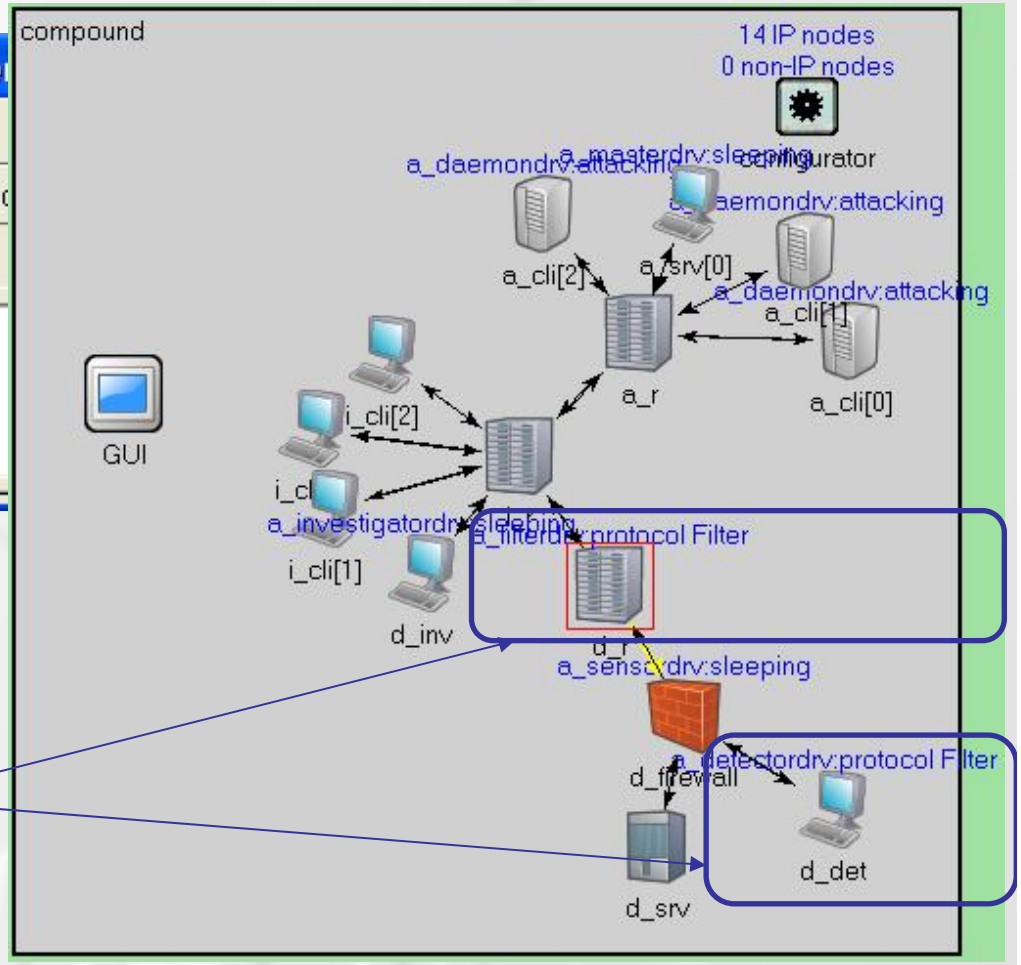


Статистика сенсора по IP адресам за 60 секунда (выделены строки с наибольшим количеством переданной информации

Сенсор посылает детектору статистику

Фазы противодействия команд агентов: (5) Действия агента «фильтр»

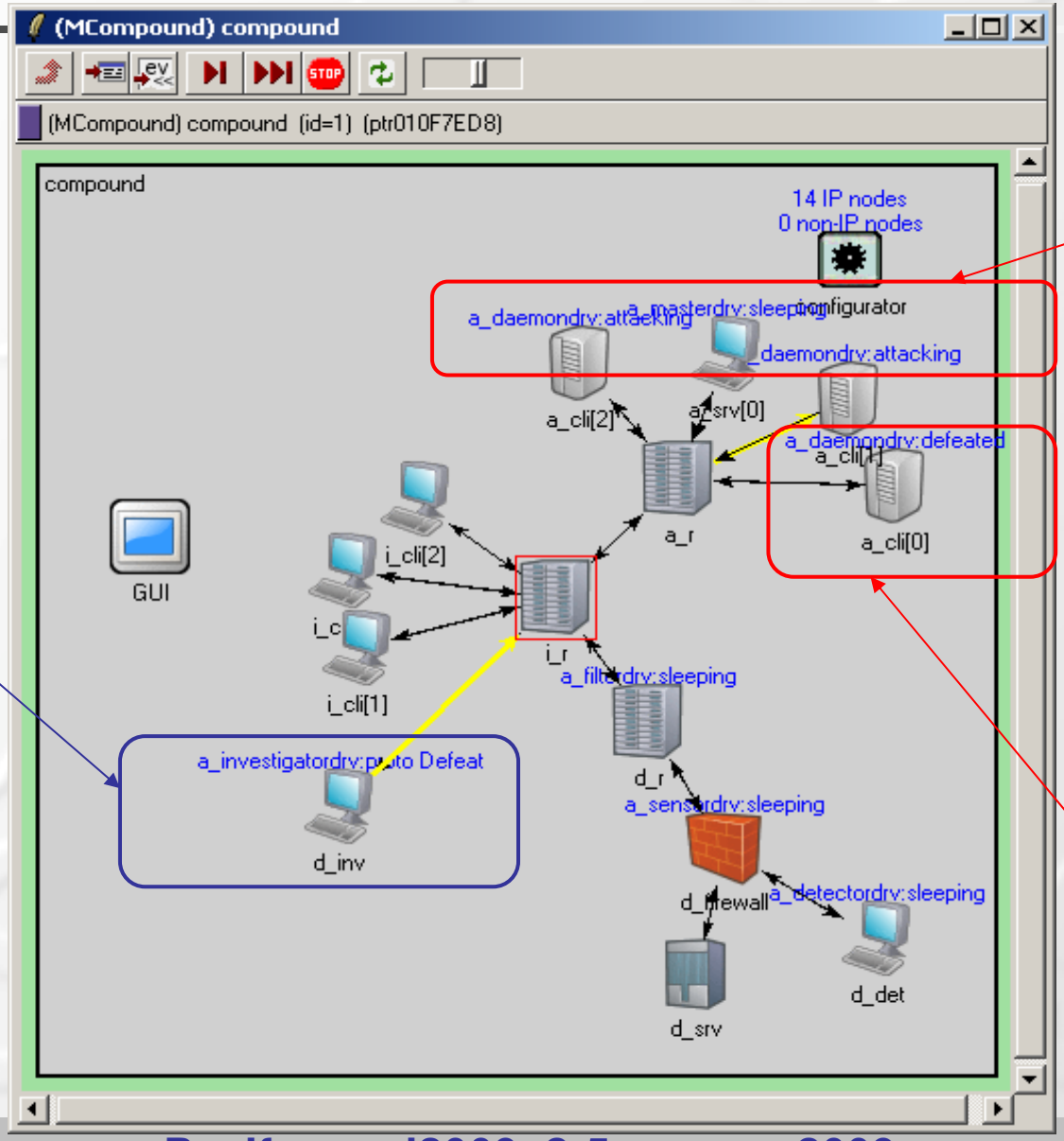




Детектор информирует «фильтра» и агента «расследования» об атаке

«Фильтр» изменяет таблицу фильтрации для пресечения атаки

Фазы противодействия команд агентов: (6) Действия агента расследования

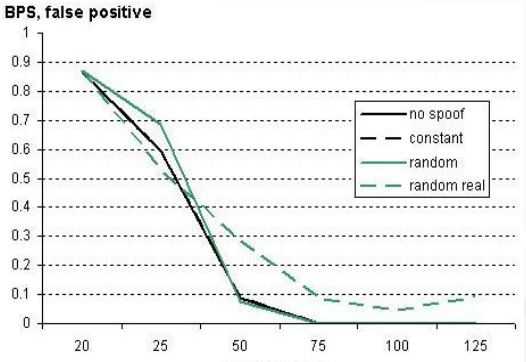


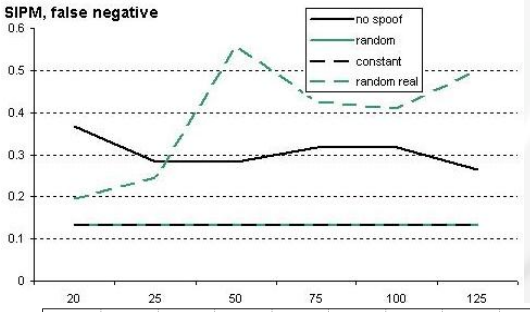
Агент «расследования» пытается обезвредить атакующих

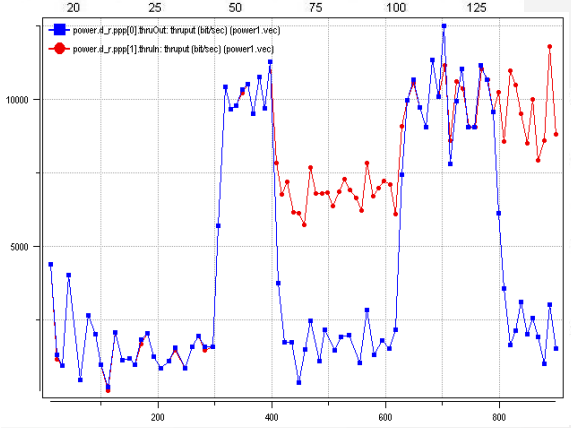
Оставшиеся «демоны» продолжают атаку

Один из «демонов» обезврежен

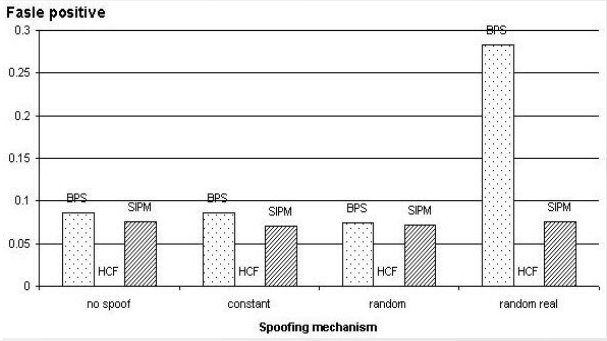
Эксперименты

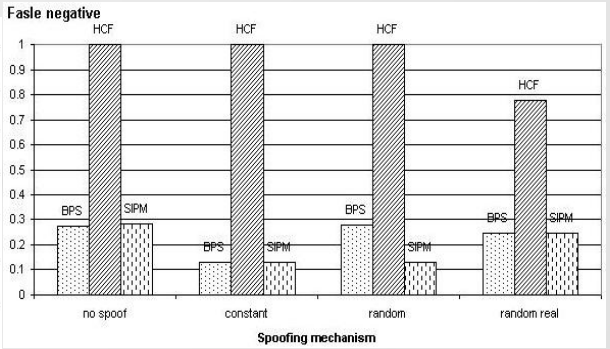






- Созданная среда моделирования позволяет проводить различные эксперименты с целью исследования стратегий реализации атак и перспективных методов защиты.
- В процессе экспериментов можно варьировать
  - топологию и конфигурацию сети;
  - структуру и конфигурацию команд атаки и защиты;
  - механизмы реализации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





Сущность режима обучения

- *В режиме обучения* формируется модель типового для исследуемой сети трафика (без реализации атаки).
- Индивидуальное обучение команд работает в соответствии с описанными методами. После начала моделирования клиенты обращаются к серверу, а он им отвечает. В это время сэмплеры регистрируют эти запросы и используют их для формирования параметров методов SIPM, HCF и BPS.
- При кооперации на уровне сэмплеров, а также при полной кооперации, команды используют данные других команд для своего обучения – в этом и заключается основное отличие *кооперативного обучения от индивидуального*.
- Зная адреса других сэмплеров, команды запрашивают данные от них, то есть данные подсетей других команд. Это дает более полную модель трафика в сети.
- При других схемах кооперации обмен данными в режиме обучения не происходит, так как эти схемы ориентированы только на кооперативную защиту.

Методы 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.

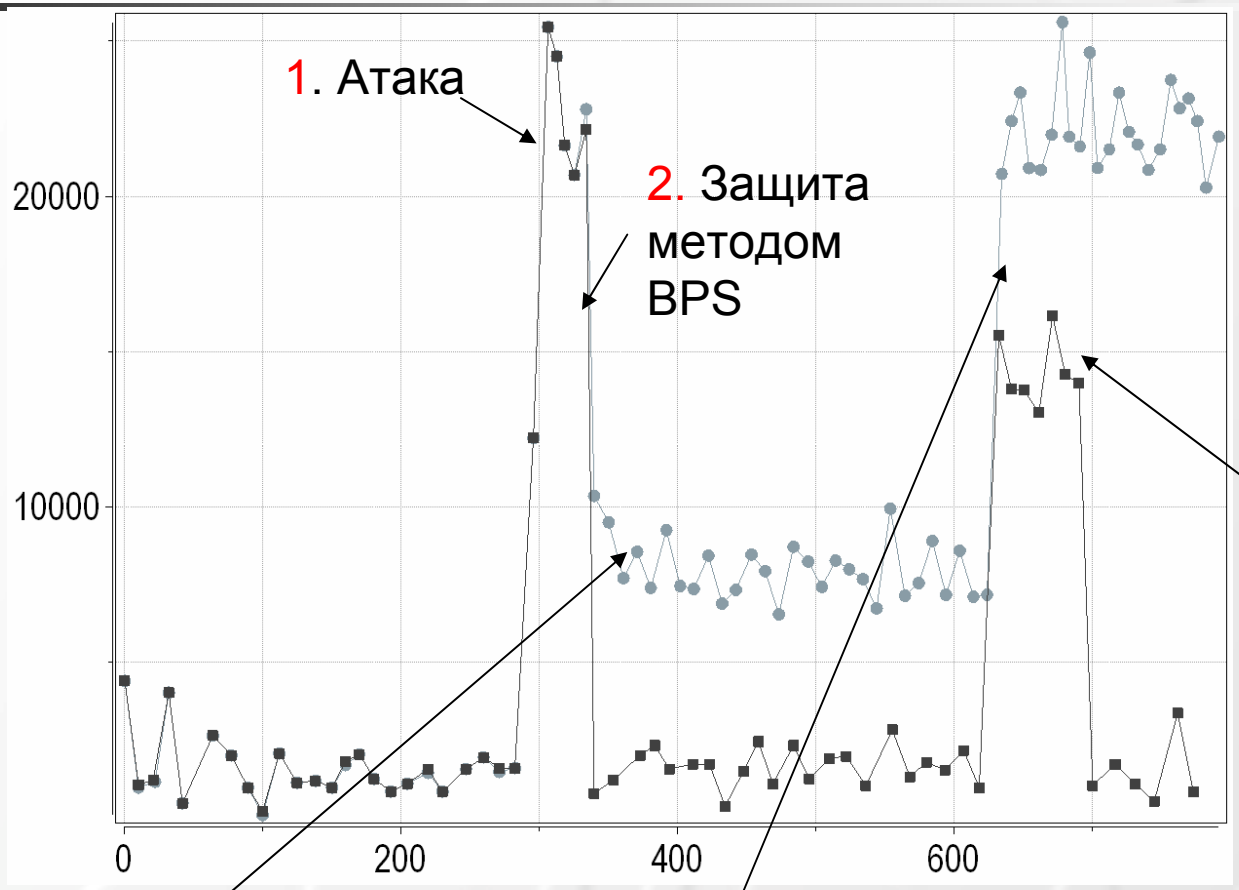
Пример базовой схемы адаптации, примененной в экспериментах

- В зависимости от мощности атаки, *команда защиты* изменяет параметры методов защиты и кооперации, минимизируя стоимость защиты. Последовательность используемых методов:

  BPS -> SIPM -> SIPM + HCF

- *Команда атаки* перераспределяет интенсивность атаки между демонами и изменяет методику подмены адреса, минимизируя количество пакетов атаки и уменьшая вероятность обезвреживания демонов агентами защиты.
  - Сначала команда, обладая большим количеством демонов, распределяет нагрузку равномерно между ними и не использует метод подмены адреса, чтобы они не были отмечены брандмауэрами своих подсетей.
  - Если, после действий команды защиты, некоторые демоны будут обезврежены, команда атаки повышает нагрузку на оставшихся (для сохранения общей интенсивности) и применяет метод подмены адреса отправителя.

Трафик при адаптации команд агентов без кооперации



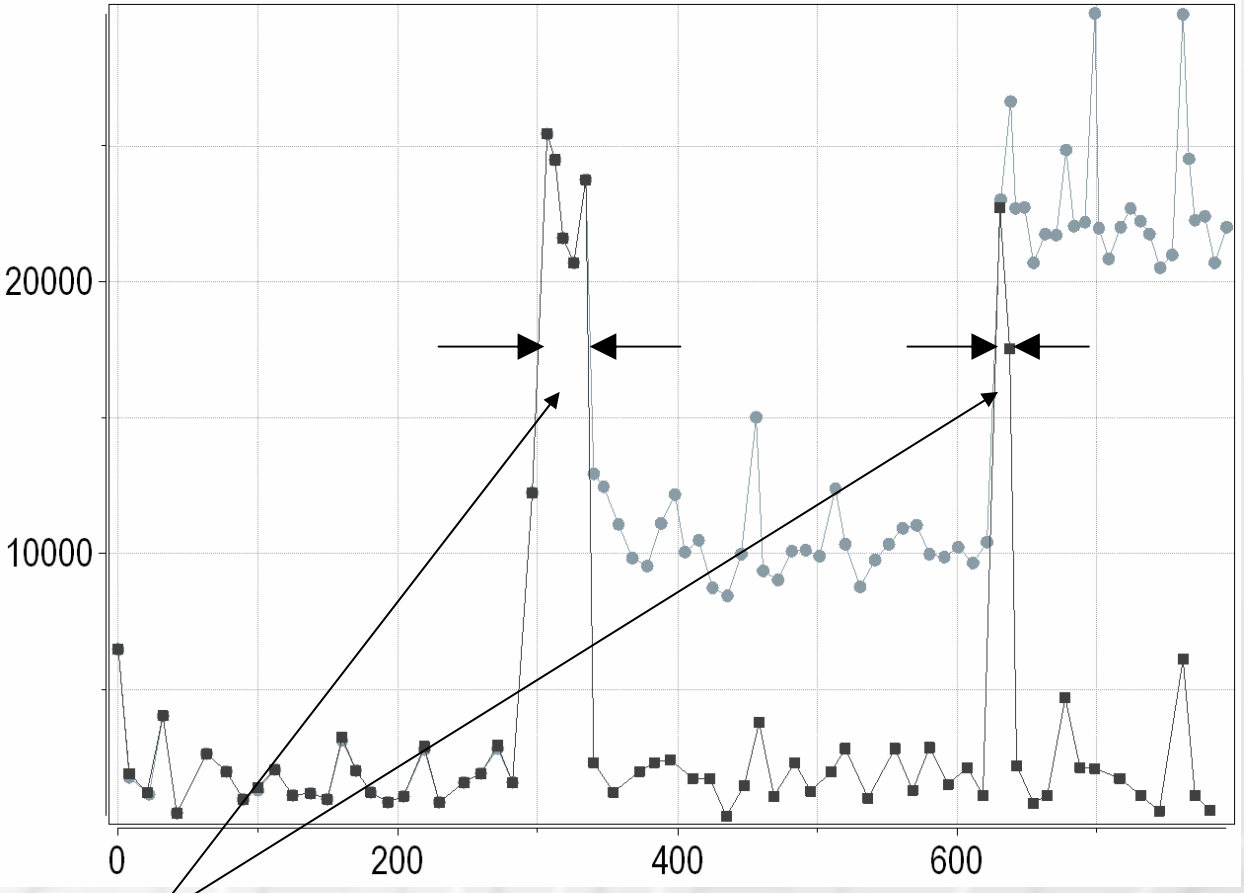
Обозначение трафика: на входе атакуемой подсети – **серый**; внутри сети - **черный**

5. Команда защиты применяет метод SIPM. Трафик внутри подсети снижается

3. Агентам защиты удается обезвредить ряд демонов, поэтому трафик на входе в защищаемую подсеть снижается

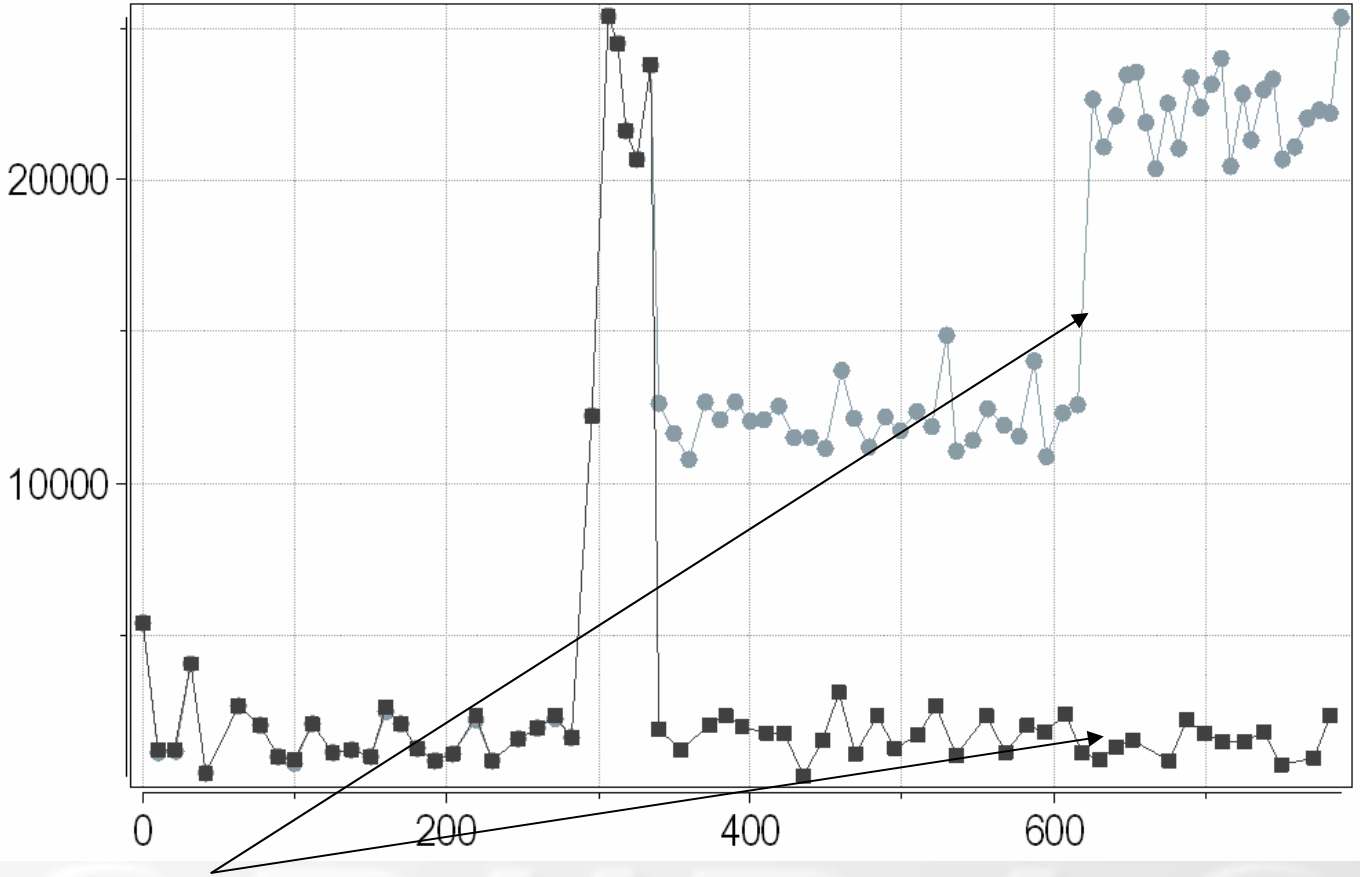
4. Мастер команды атаки перераспределяет нагрузку на оставшихся демонов и меняет метод подмены адреса на “случайный”. Из-за этого сильно возрастает трафик

Трафик при адаптации команд агентов при кооперации на уровне фильтров



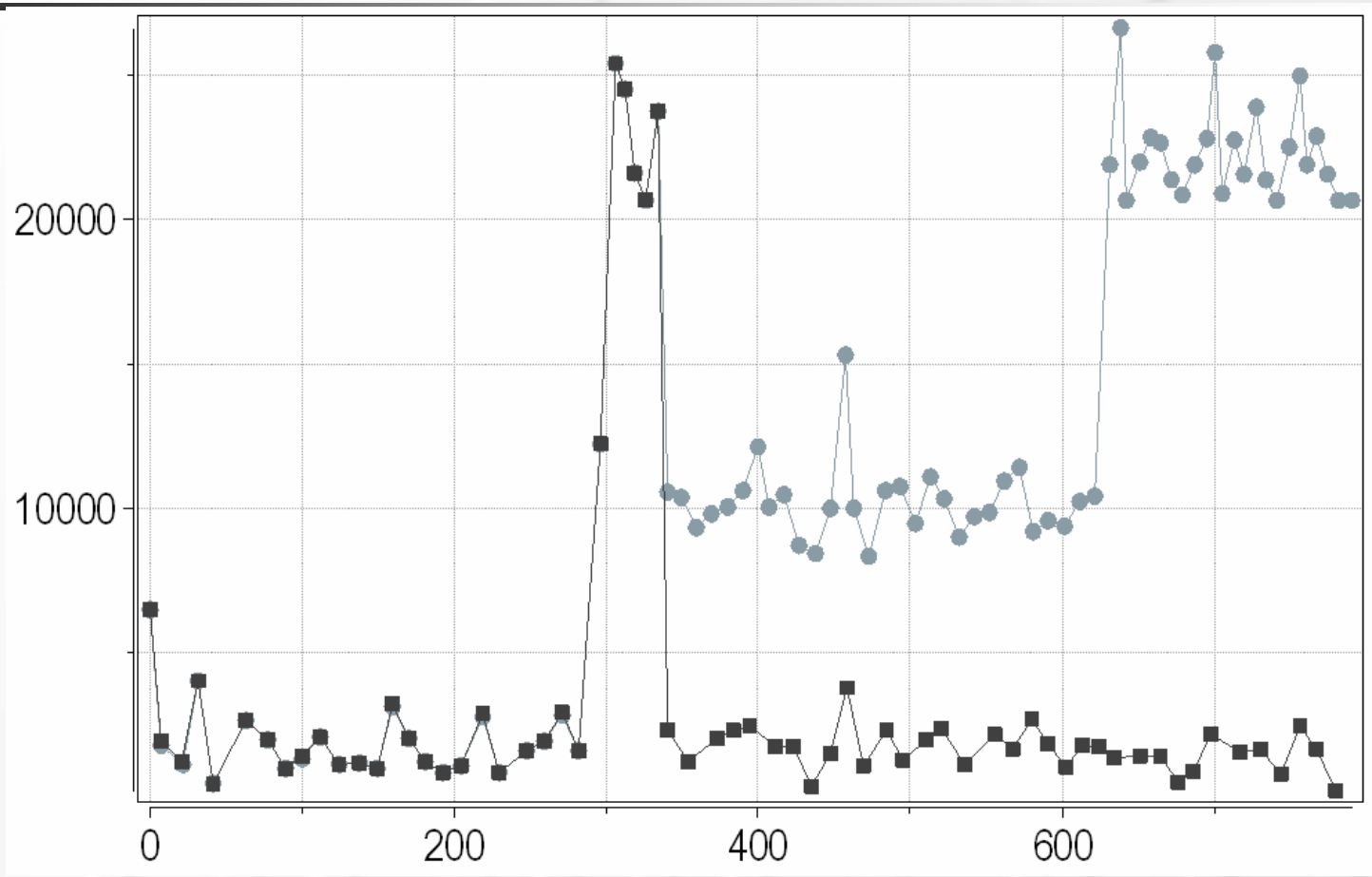
Благодаря тому, что команда защиты получает правила фильтрации от других команд, блокировка трафика атаки происходит существенно быстрее, чем без кооперации

Трафик при адаптации команд агентов при кооперации на уровне сэмплеров



При изменении метода атаки растет только трафик на входе в защищаемую подсеть. Внутри подсети трафик остается на приемлемом уровне. Это связано с тем, что при обучении, команды защиты получали данные от сэмплеров других команд из других подсетей. Этих данных оказалось достаточно для метода SIPM, чтобы сразу блокировать атакующих, изменяющих свой адрес на случайный.

Трафик при адаптации команд агентов при полной кооперации



Трафик имеет такой же характер, что и при кооперации на уровне сэмплеров. Решающую роль в защите от атаки, сыграла кооперация сэмплеров.

Основные результаты работы (1)

- Представлен подход к исследованию адаптивных и кооперативных механизмов функционирования команд интеллектуальных агентов атаки и защиты
- Возможности подхода анализировались на основе моделирования перспективных механизмов защиты от атак DDoS.
- На базе OMNeT++ INET Framework разработана среда для многоагентного моделирования.
- Проведено большое количество экспериментов. Исследовались параметры эффективности адаптивной кооперативной защиты

Основные результаты работы (2)

- Проведенные эксперименты показали возможность использования предложенного подхода для моделирования механизмов защиты и для анализа проектируемых сетей.
- Они продемонстрировали также, что использование кооперации нескольких команд и комбинированного адаптивного применения различных механизмов функционирования ведет к существенному повышению эффективности защиты.
- Дальнейшее направление исследований связано с более глубоким анализом эффективности кооперативных механизмов различных команд, совершенствованием механизмов адаптации и самообучения агентов, расширением библиотек атаки и защиты, анализом новых механизмов защиты

Контактная информация

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

Благодарности

- Разработчики программной среды и приложений: Уланов А.В., Алексеев А.С., Коновалов А.М. и др.
- Работа выполняется при финансовой поддержке РФФИ (проект №07-01-00547) и программы фундаментальных исследований ОНИТ РАН.

РОССИЙСКАЯ АКАДЕМИЯ НАУК