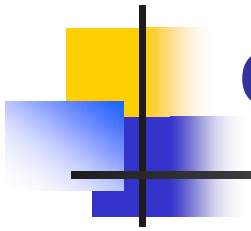
Проактивные механизмы защиты от быстро распространяющихся сетевых червей

И.В. Котенко

НИГ компьютерной безопасности

Санкт-Петербургский институт информатики и автоматизации РАН (СПИИРАН)

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



Содержание

- Задача исследования
- Предложенный подход
- Механизмы обнаружения и реагирования
- Архитектура средств моделирования
- Реализация
- Подход к комбинированию
- Методика моделирования и сценарии экспериментов
- Результаты экспериментов и анализ
- Заключение

Задачи исследования

- Разработка **проактивного подхода к защите от сетевых червей**, базирующегося на использовании механизмов обнаружения и ограничения интенсивности соединений сетевых червей
- Создание **моделей, методик и программно-аппаратного средства (стенда) для исследования механизмов защиты от сетевых червей** на основе моделирования различных типов и экземпляров сетевых червей и механизмов защиты от них
- **Исследование механизмов обнаружения и сдерживания сетевых червей**, которые направлены на быстро распространяющихся червей

Назначение и сущность подхода

- **Предлагаемый подход предназначен** для обнаружения (агрессивных) сетевых червей (посредством выявления их действий по сканированию уязвимых хостов) и сдерживания их дальнейшего распространения (за счет ограничения и блокирования посылаемых инфицированными узлами сетевых пакетов)
- **Проактивность** <-> реактивность
- **Проактивное обнаружение и ограничение интенсивности установления сетевых соединений основано** на *автоматических механизмах использования информации об "истории" анализируемых сетевых событий и прогнозе будущих событий, а также автоматической подстройке параметров обнаружения сетевых червей и ограничения трафика к текущему состоянию конфигурации сети и обрабатываемого трафика*

Основные требования к механизмам защиты

- **адекватность:** должны обеспечиваться низкие показатели пропуска атаки и ложного срабатывания
- **оперативность:** вредоносная сетевая активность должна обнаруживаться как можно раньше, данное требование напрямую влияет на величину ущерба, приносимого в результате эпидемии сетевых червей
- **эффективность использования системных ресурсов** и возможность реализации на сетевом оборудовании
- **автоматическое выполнение:** разрабатываемые механизмы должны функционировать без вмешательства (или при минимальном вмешательстве) администратора
- **возможность обнаружения** (кроме **быстро сканирующих сетевых червей**) также "медленных" червей, использующих скрытные алгоритмы сканирования

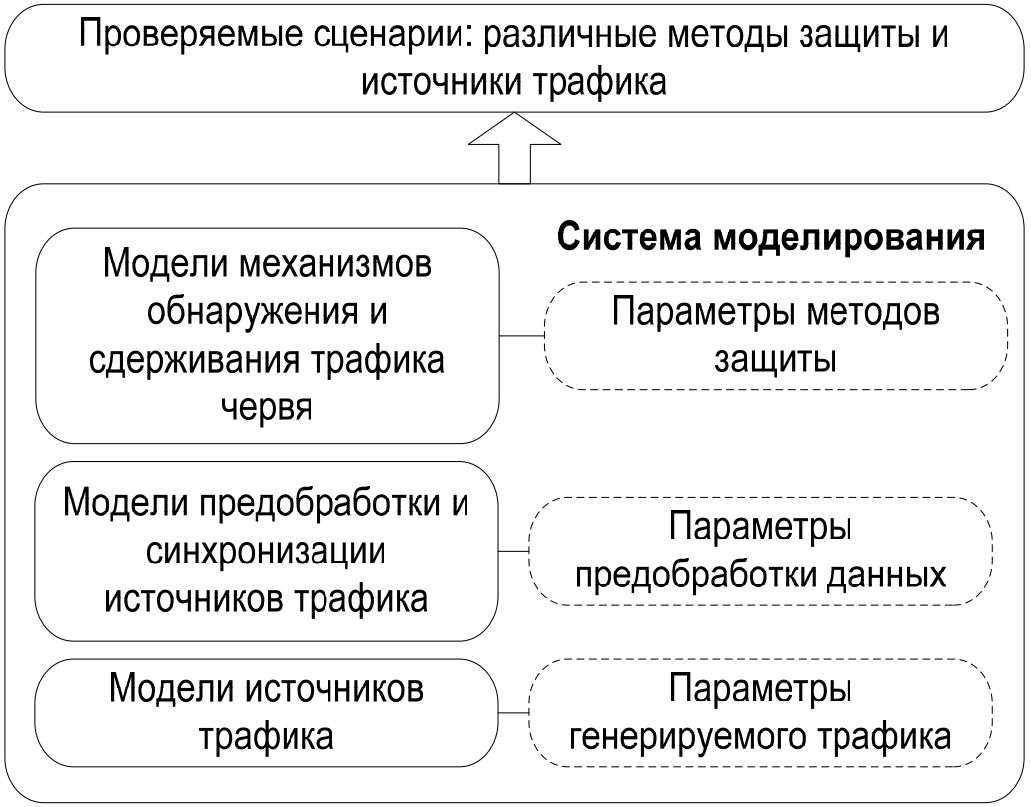
Особенности предлагаемых проактивных механизмов защиты

- **(1) "Многорезолюционность":** использование нескольких интервалов времени ("окон") наблюдения сетевого трафика и различных порогов для отслеживаемых параметров
- **(2) Гибридность:** применение различных механизмов защиты, основанных на разных алгоритмах и математических методах, в том числе учитывающих события, характеризующие как аномальную, так и нормальную сетевую активность хоста
- **(3) Многоуровневое комбинирование механизмов защиты** (как системы базовых классификаторов и мета-классификатора)
- **(4) Адаптивность:** приспособление параметров обнаружения и ограничения трафика к текущему состоянию конфигурации сети и трафика

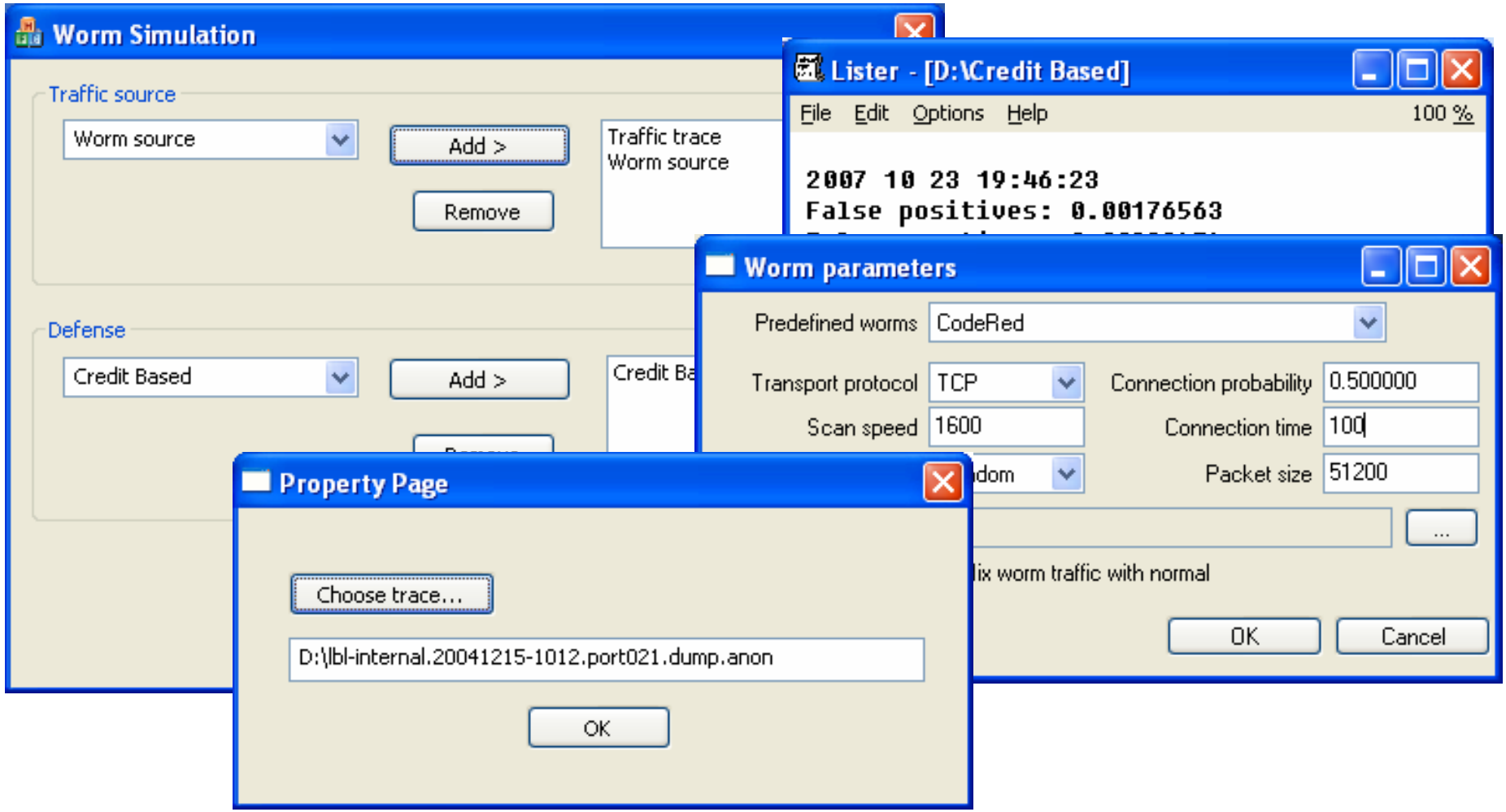
Обобщенная архитектура системы моделирования

Архитектура средств моделирования

- **Базовые компоненты:**
  - Генератор трафика существующих червей
  - Генератор трафика новых червей
  - Система предобработки и синхронизации источников трафика (для приведения трафика из формата источников в формат, удобный для анализа механизмами защиты, синхронизации нескольких источников трафика и передачи трафика механизмам защиты в упорядоченном во времени виде)
  - Исследуемые механизмы защиты

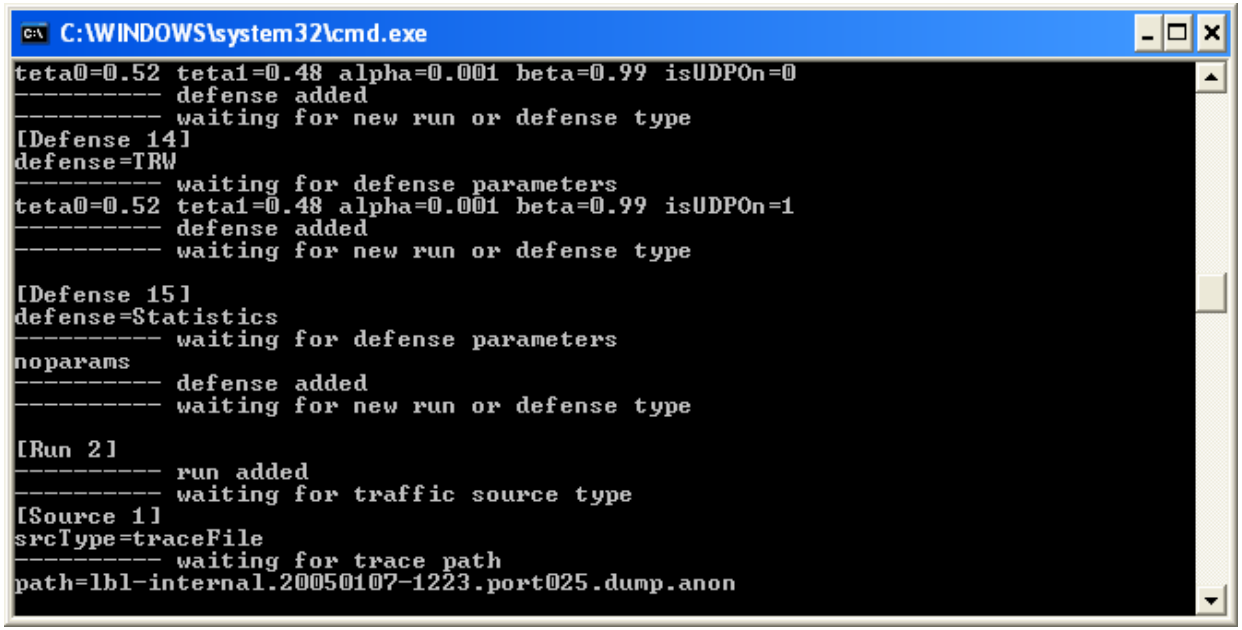


Интерфейс программного комплекса моделирования



Консольное приложение

- Предназначено для пакетного запуска большого количества экспериментов
- В качестве параметра передается имя файла со скриптом, содержащим набор конфигураций для запусков экспериментов.



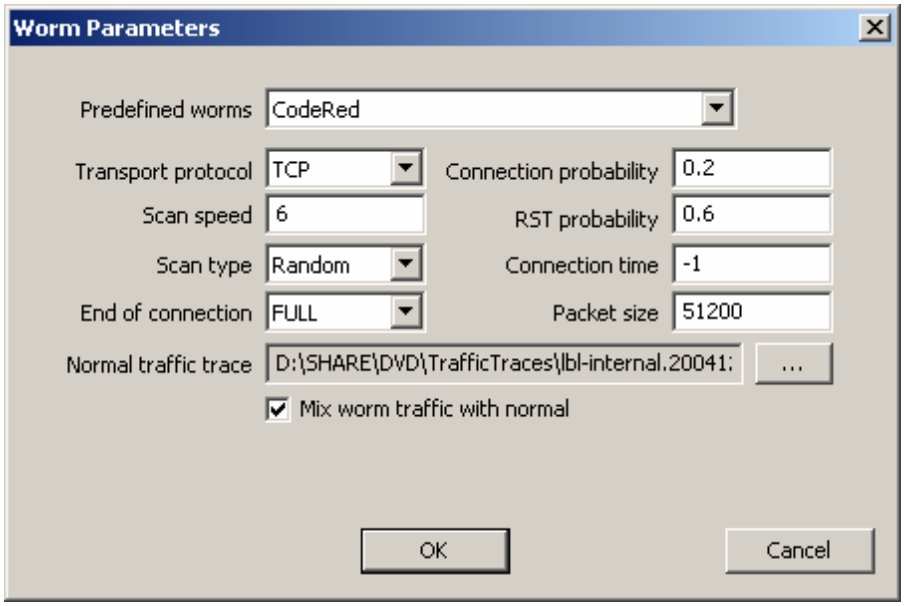
console.exe run_exp_all.txt

Использованные записи трафика

- *Трафик, содержащийся в [LBNL/ICSI Trace]*, включает более 100 часов записи трафика сети уровня предприятия за период с октября 2004 по январь 2005 года. Содержание трафика описано в [Pang et al., 05].
- *Трафик, представленный в [GRID],* содержит записи трафика, зафиксированного на границе сети университета Наполи (University of Napoli) “Federico II” и сети Интернет.
- *Трафик, содержащийся в [LIP6],* включает записи трафика, сделанные при помощи PPLive в сети Парижского Университета Пьера и Марии Кьюри (Pierre & Marie Curie University (UPMC)) во время он-лайн трансляции матча Италия-Украина во время Чемпионата мира по футболу 2006 г.
- *Собственные записи трафика* содержат записи трафика p2p-приложений, зафиксированные на испытательном стенде, созданном для целей проекта.

Генератор трафика

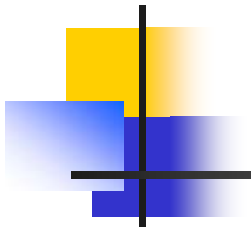
- Способен формировать
  - как нормальный трафик (на основе “проигрывания” ранее записанного трафика
  - так и трафик различных типов сетевых червей, как ранее известных, так и неизвестных



- *Деятельность ранее известных червей моделируется* путем задания предопределенных параметров функционирования, соответствующих известным червям
- *Действия новых червей моделируются* на основе задания произвольных параметров функционирования сетевых червей

Основные параметры генератора для моделирования новых червей

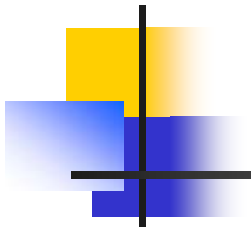
- protocol — тип протокола транспортного уровня, используемого сетевым червем (UDP или TCP);
- scanSpeed — скорость сканирования (пакетов в секунду);
- scanType — способ получения IP-адреса сканируемого хоста (хоста-жертвы) или тип сканирования (RANDOM, SEQUENTIAL, PERMUTATION, PARTITION, LOCAL, TOPOLOGICAL);
- end_of_connection_t — способ завершения TCP соединений (FULL, SHORT);
- connProb — вероятность успешного соединения, в случае TCP – это ответный пакет SYN ACK, в случае UDP – ответный пакет UDP;
- rstProb — вероятность ответа TCP-RST в случае неудачного соединения;
- connTime — время соединения (в секундах);
- packetSize — размер генерируемого пакета (в байтах);
- tracePath — файл с трафиком для смешивания;
- isMixTraffic — использовать или нет параметры трафика для генерации трафика червя.



Классы механизмов

Применяемые классы механизмов:

- “дросселирование/регулирование вирусов” (“virus throttling”)
- на основе данных о неудачных соединений (“failed connection”)
- на базе “порогового случайного прохождения” (Threshold RandomWalk)
- на базе упрощенного “порогового случайного прохождения” (Simplified Threshold RandomWalk)
- На основе кредитов доверия (“Credit-based rate limiting”)
- на основе DNS-статистики (“DNS-based rate limiting”)



Комбинирование механизмов (1/2)

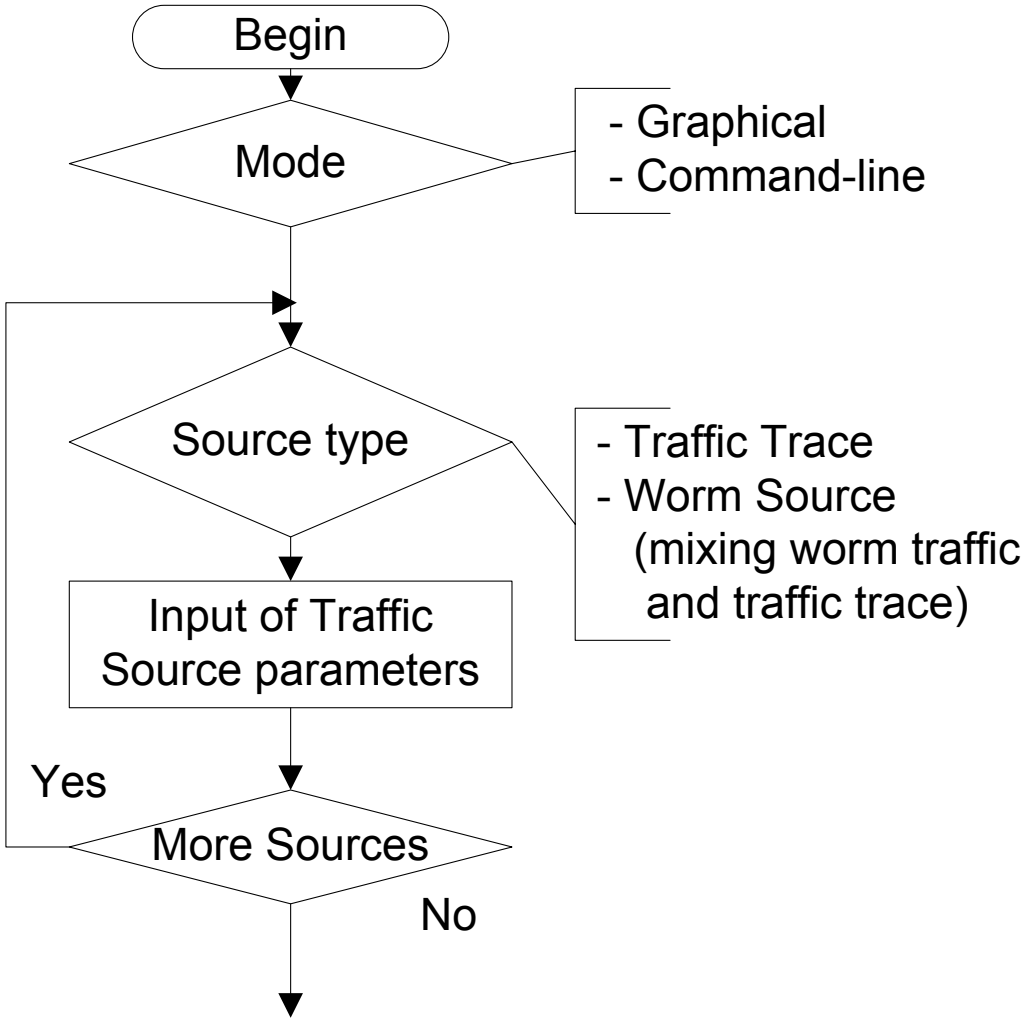
- Комбинирование данных механизмов заключается:
  - в выборе отдельных методов, которые наилучшим образом работают в текущих условиях, или
  - в использовании нескольких механизмов (как различных классов, так и одного класса, но с отличающимися параметрами), и формировании заключения о наличии сетевого червя на основе обработки заключений каждого механизма с различными весами.

Комбинирование механизмов (2/2)

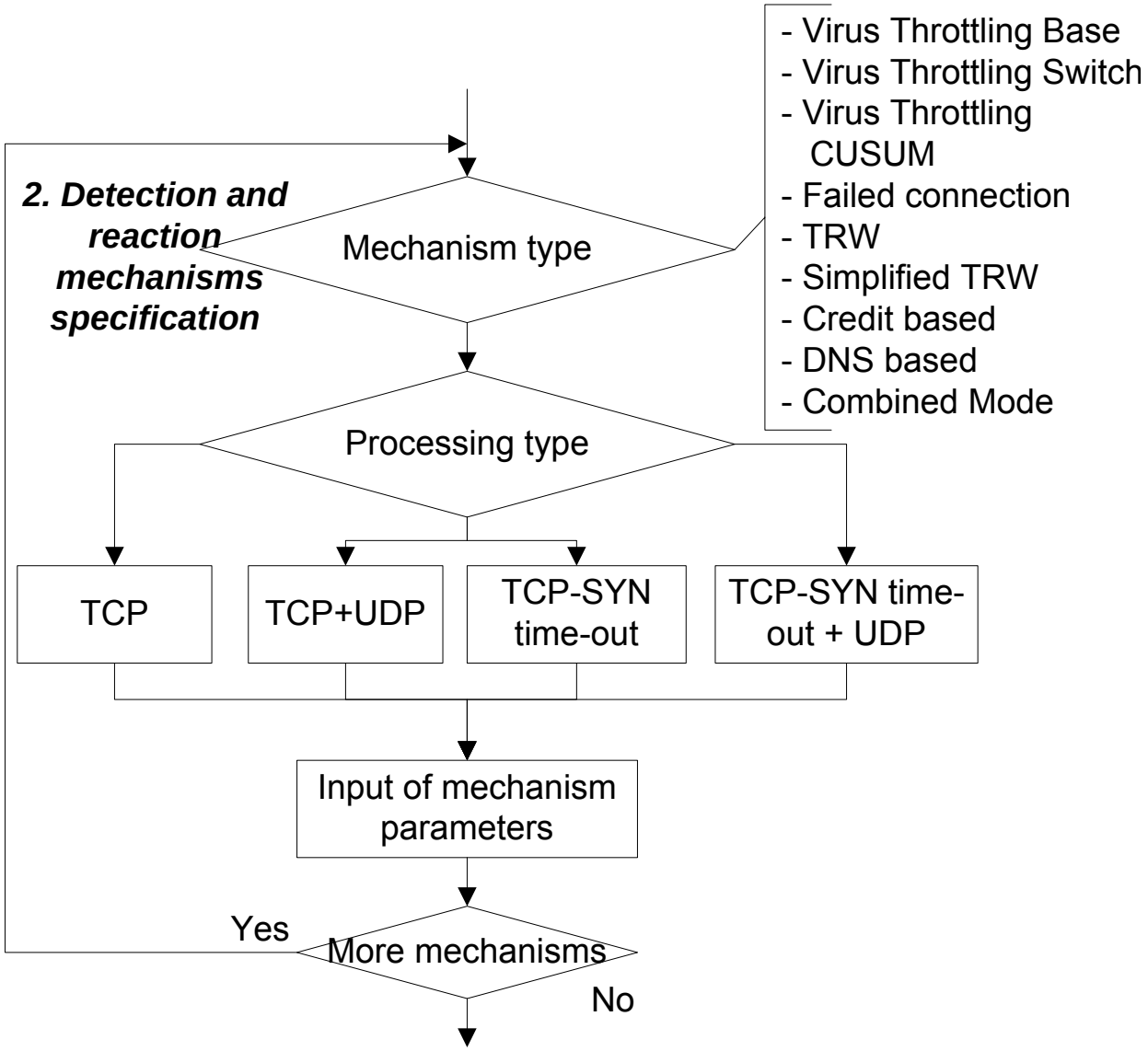
- Выбраны четыре основных параметра трафика:
  - средняя частота приходящих пакетов;
  - процент TCP SYN-запросов;
  - среднее количество пакетов на один хост-источник;
  - процент успешных соединений.
- Функция вычисления коэффициентов применимости *W*(*d*,*x1*,…,*xn*) принимает в качестве аргументов тип (класс) *d* механизма защиты и точку декартова *n*-мерного гиперпространства, заданного параметрами (в указанном примере — четырехмерного) – (*x1, x2, x3, x4*).

Методика моделирования (1/3)

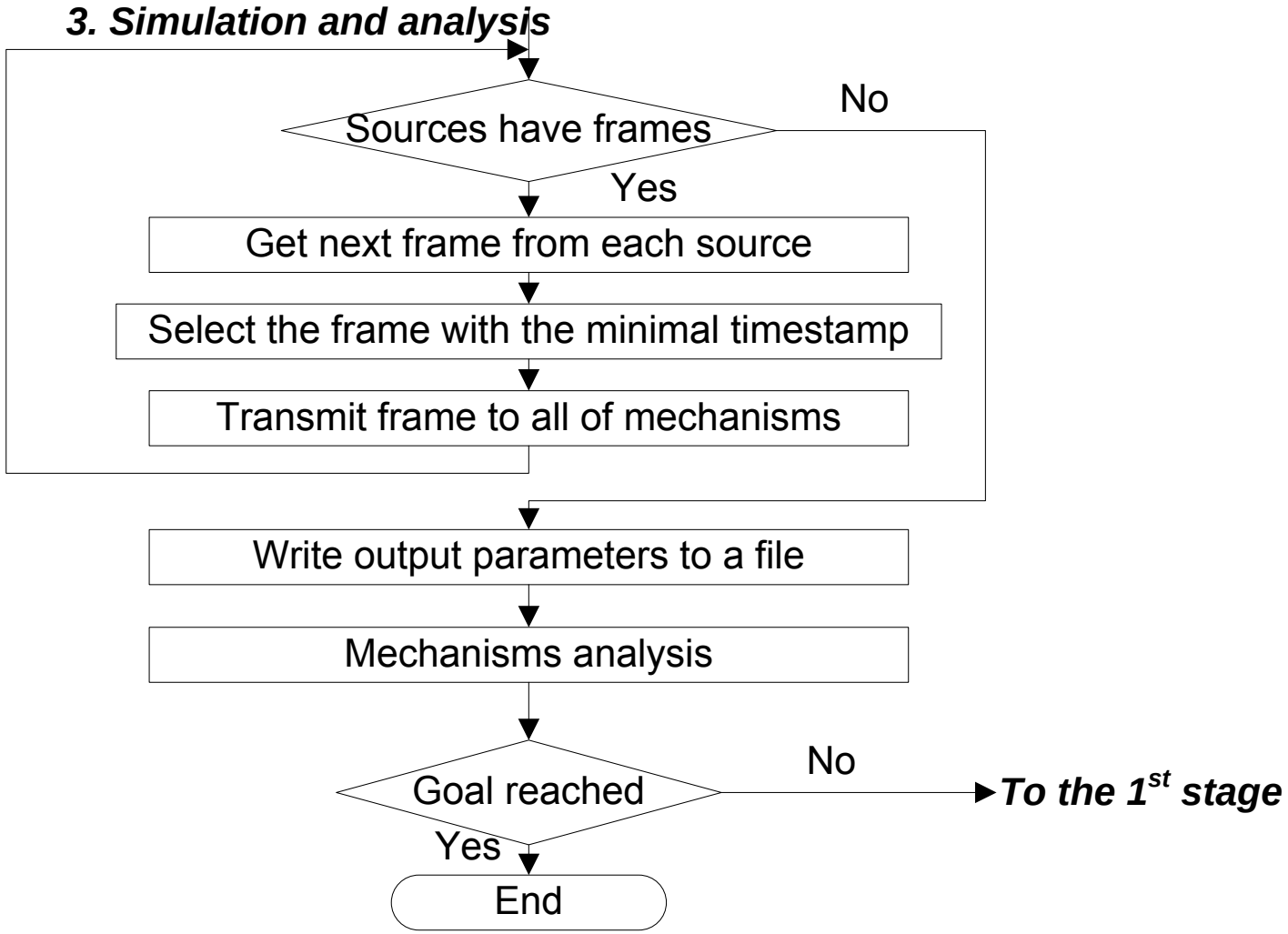
1. Traffic Sources specification



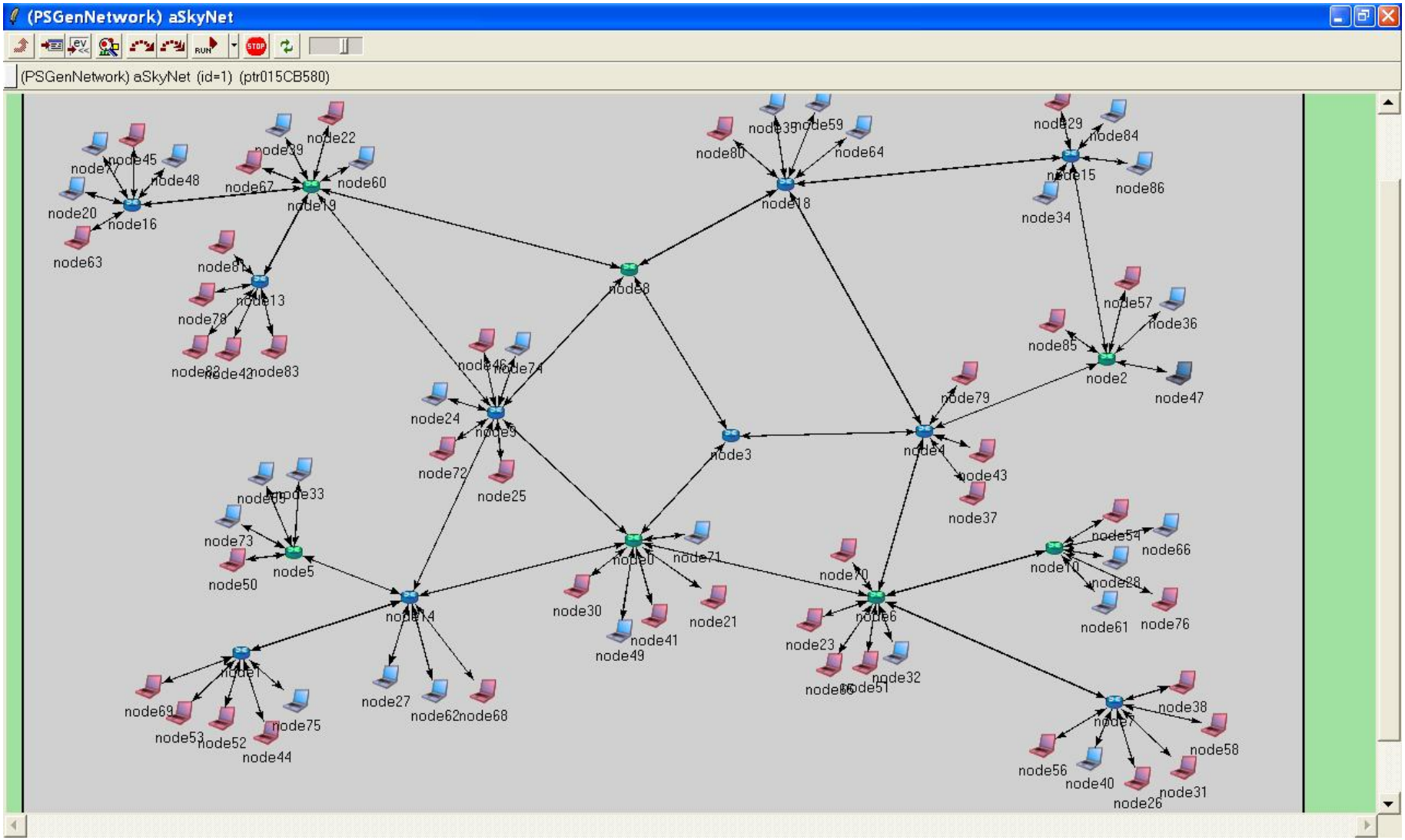
Методика моделирования (2/3)

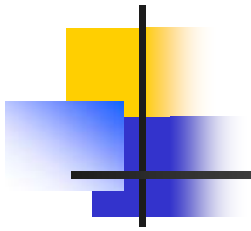


Методика моделирования (3/3)



Пример моделирования распространения червя в сети

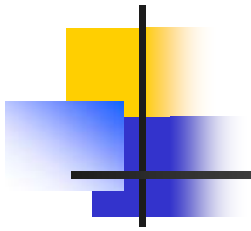




Анализ

Для оценки и сравнения механизмов обнаружения и противодействия используются следующие параметры:

- процент ложных срабатываний;
- процент пропуска атак;
- время реакции метода;
- количество обработанных пакетов;
- минимальное время обработки пакета;
- максимальное время обработки пакета;
- среднее время обработки пакета;
- максимальный объем памяти, используемый при выполнении механизма;
- количество обращений к памяти, осуществляемое при выполнении механизма;
- количество записей в память, осуществляемое при выполнении механизма;
- показатель точности метода.



Эксперименты

- Использовались трафики с низким и высоким процентом P2P-приложений.
- Всего было использовано **7 нормальных трафиков**, к трем из которых подмешивались соответствующие записи сканеров, и **5 P2P-трафиков**. Более подробное описание трафиков см. п. 2.4.1. отчета.
- Все трафики смешивались с червями трех видов:
  - Code Red II,
  - Slammer и
  - искусственный червь.
- Кроме того, механизмы защиты исследовались на всех указанных трафиках без примеси червя и на чистых трафиках червя.
- Всего было проведено около 700 экспериментов.
- Для каждого механизма защиты использовались оптимальные параметры, полученных по результатам экспериментов с отдельными методами.

Выходные параметры механизмов (нормальный трафик с исск. червем)

№ п/п	Механизм	Среднее значение суммы ошибок	Среднее значение коэффициента ложных срабатываний (FP)	Среднее значение коэффициента пропусков атак (FN)
1	TRW	0,007396	0,004980	0,002416
2	VT-S	0,023940	0,023300	0,000663
3	VT-C	0,024648	0,024100	0,000530
4	CB	0,025969	0,025600	0,000344
5	FC-B	0,063966	0,009680	0,054291
6	DNS	0,985548	0,075500	0,230215

Классы памяти	Механизмы, в порядке возрастания суммы ошибок					
Экономный	VT-S	VT-C				
Экономный+Средний	VT-S	VT-C	CB	FC-B	DNS	
Экономный+Средний+ Расточительный	TRW	VT-S	VT-C	CB	FC-B	DNS

Выходные параметры механизмов (нормальный трафик с Code Red II)

№ п/п	Механизм	Среднее значение суммы ошибок	Среднее значение коэффициента ложных срабатываний (FP)	Среднее значение коэффициента пропусков атак (FN)
1	CB	0,027848	0,025692	0,002156
2	VT-S	0,032513	0,023277	0,009236
3	VT-C	0,033346	0,024118	0,009228
4	TRW	0,069142	0,004980	0,064162
5	FC-B	0,071842	0,037267	0,034575
6	DNS	0,997316	0,772736	0,224579

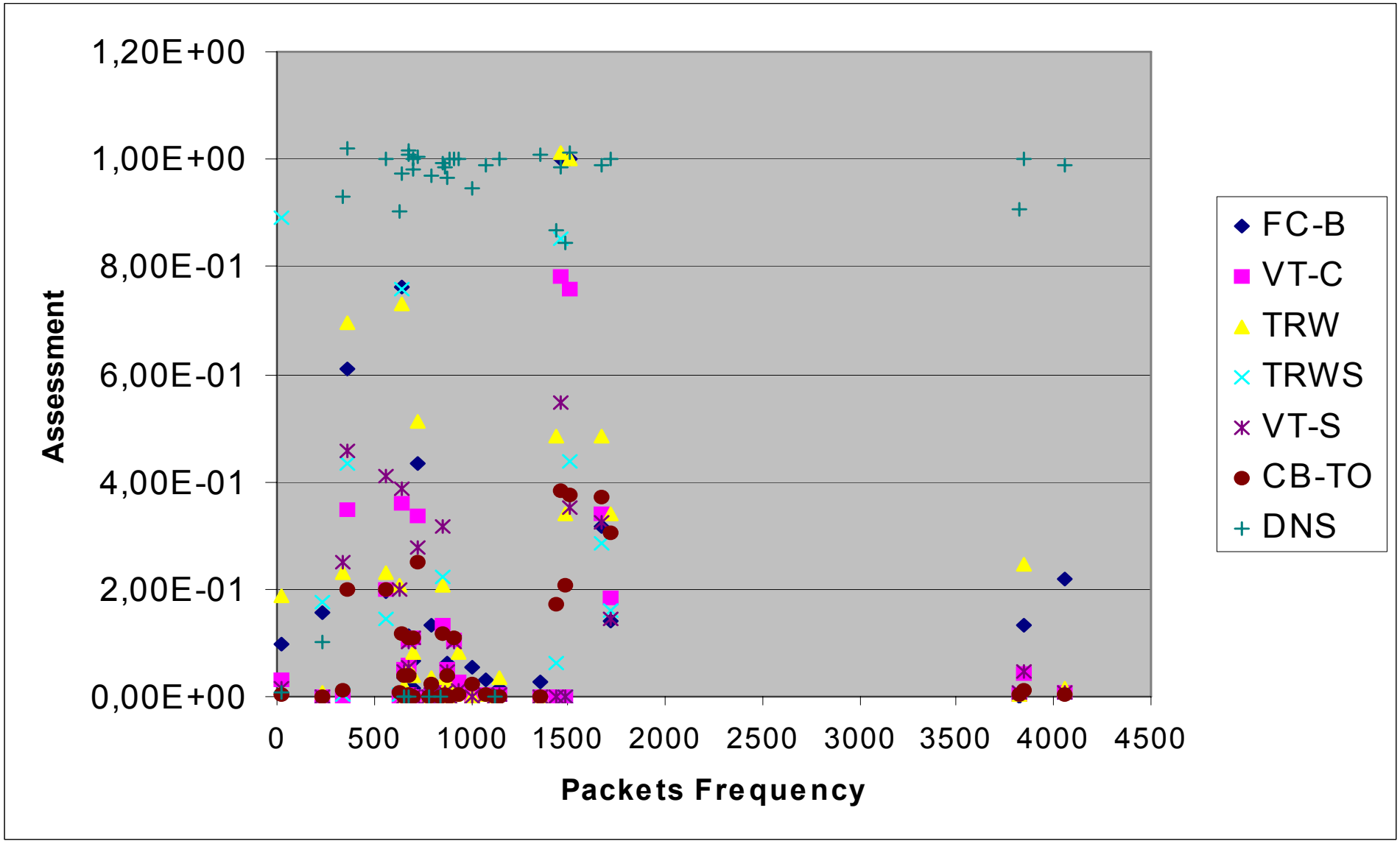
Классы памяти	Механизмы, в порядке возрастания суммы ошибок					
Экономный	VT-S	VT-C				
Экономный+Средний	CB	VT-S	VT-C	FC-B	DNS	
Экономный+Средний+ Расточительный	CB	VT-S	VT-C	TRW	FC-B	DNS

Выходные параметры механизмов (P2P трафик с Code Red II)

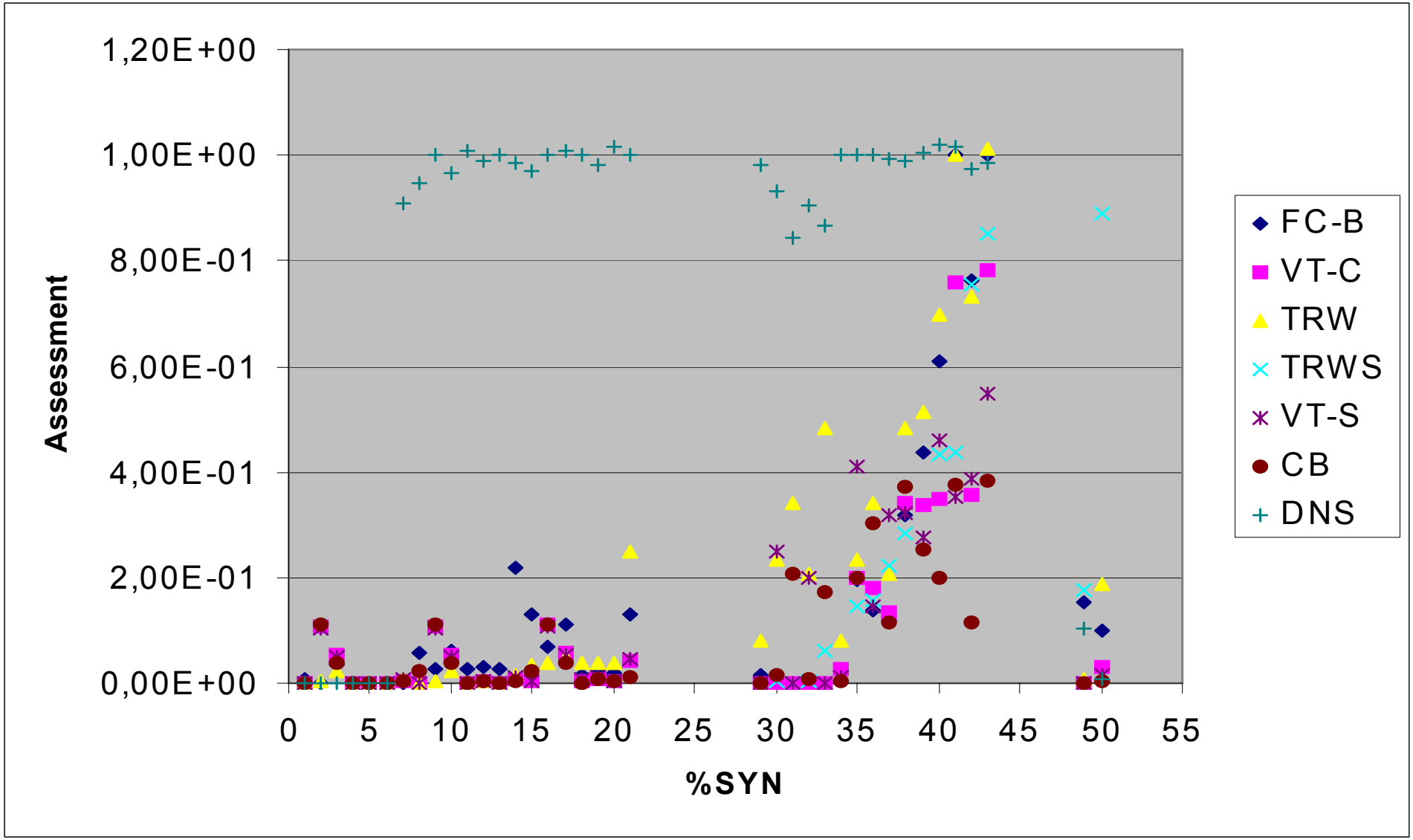
№ п/п	Механизм	Среднее значение суммы ошибок	Среднее значение коэффициента ложных срабатываний (FP)	Среднее значение коэффициента пропусков атак (FN)
1	CB	0,265824	0,265395	0,000429
2	VT-S	0,404845	0,208435	0,196409
3	VT-C	0,517375	0,067945	0,449429
4	TRWS	0,619064	0,115654	0,503410
5	FC-B	0,761482	0,031890	0,729592
6	TRW	0,790602	0,170161	0,620441
7	DNS	0,999529	0,929318	0,070211

Классы памяти	Механизмы, в порядке возрастания суммы ошибок						
Экономный	VT-S	VT-C					
Экономный+Средний	CB	VT-S	VT-C	FC-B	DNS		
Экономный+Средний+ Расточительный	CB	VT-S	VT-C	FC-B	TRWS	TRW	DNS

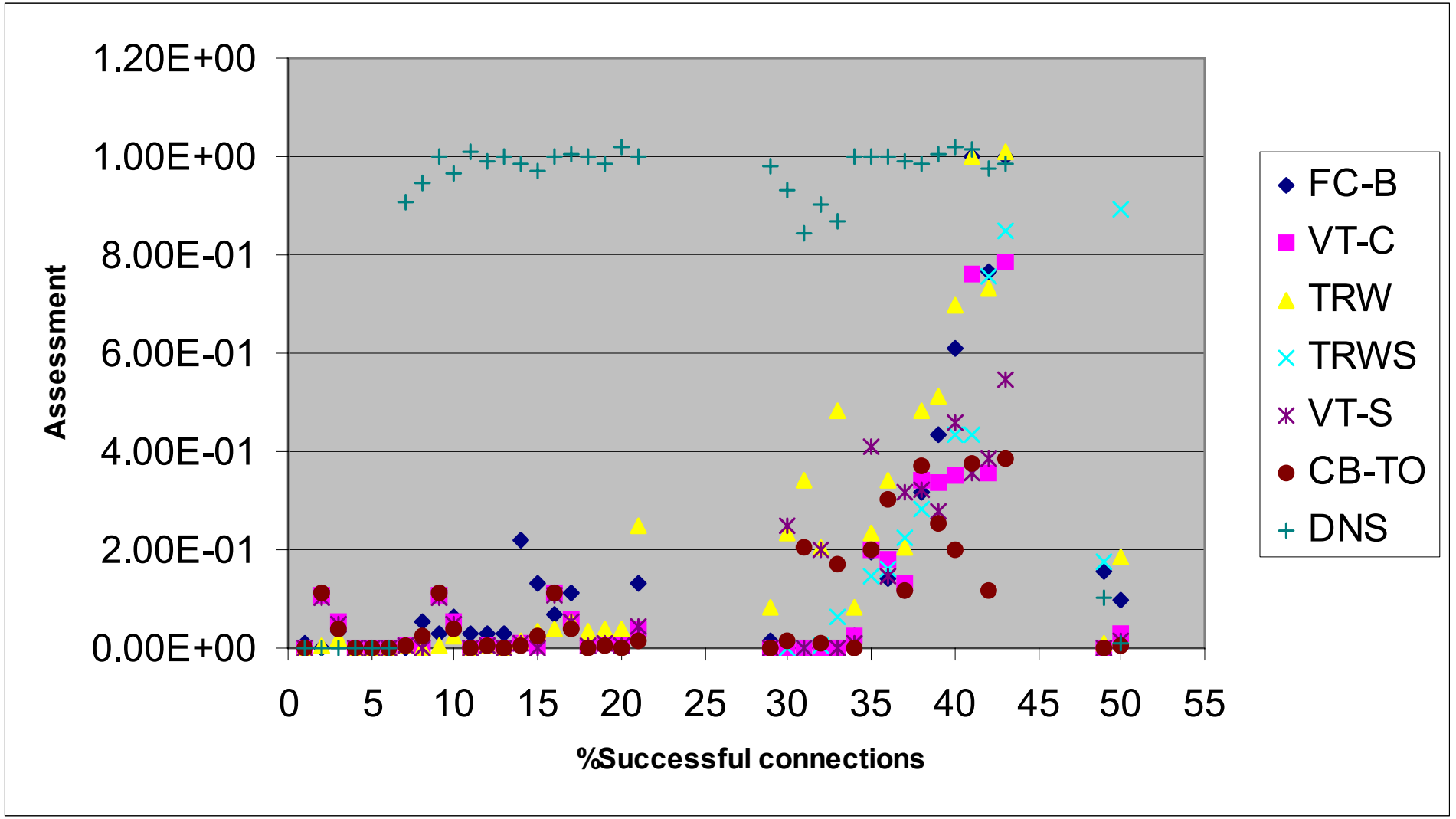
Зависимость значения суммы ошибок методов от частоты пакетов (для всех трафиков)

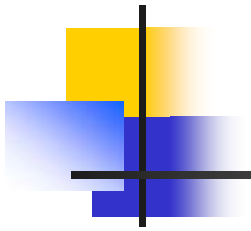


Зависимость значения суммы ошибок методов от процента TCP-SYN пакетов (для всех трафиков)



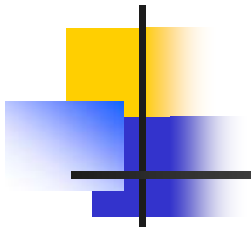
Зависимость значения суммы ошибок методов от процента успешных соединений (для всех трафиков)





Текущая и дальнейшая работа

- Совершенствование предложенных и реализованных механизмов защиты и подхода в целом.
- Применение методов машинного обучения: составить и исследовать пространство признаков на основе существующих работ в этой области и использовать отдельные признаки в исследуемых механизмах.
- Реализация механизмов адаптации: При изменении мощности атаки, подсистема адаптации выбирает конфигурацию системы защиты так, чтобы оптимизировать функцию эффективности.
- Использование различных схем кооперации механизмов защиты: на уровне сенсора, детектора, фильтра
- Исследование возможных будущих червей и механизмов защиты от них



Заключение

- Предложен проактивный подход к защите от сетевых червей, базирующийся на использовании механизмов обнаружения и сдерживания распространения сетевых червей
- Предложен подход к исследованию механизмов обнаружения и сдерживания распространения сетевых червей
- Разработан программный комплекс моделирования механизмов защиты
  - Реализован генератор трафика червя
  - Реализованы механизмы обнаружения и реагирования
  - Реализованы средства моделирования
- Проведены эксперименты
- Сформулированы рекомендации по применяемым механизмам, их улучшению и дальнейшей работе.

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 проекта с фирмой Hewlett-Packard и проекта Евросоюза RE-TRUST (контракт № 021186-2).

РОССИЙСКАЯ АКАДЕМИЯ НАУК