Агентно-ориентированное моделирование бот-сетей

Шоров А.В., Котенко И.В.

Санкт-Петербургский институт информатики и автоматизации РАН

Коновалов А.М.

ЗАО “Аркадия”

РусКрипто’2010 , 1 - 4 апреля 2010 г.

Содержание

- Введение
- Релевантные работы
- Сущность и особенности задачи моделирования бот-сетей
- Комплекс моделирования
- Эксперименты
- Заключение

Введение

С появлением бот-сетей злоумышленники получили доступ к миллионам зараженных компьютеров пользователей, а число киберпреступлений увеличилось в сотни раз.

По данным ФБР за октябрь 2009 г., потери из-за бот-сетей составили около $100 млн.

Спектр применения бот-сетей довольно обширен: кража конфиденциальных данных (кража денег с электронных счетов, номеров кредитных карт, и т.д.), организация рассылки спама, принудительный показ рекламы, организация атак DDoS, использование вычислительной мощности инфицированных компьютеров в своих целях, компрометация легитимных пользователей, обман систем отслеживания рейтинга (например, атака типа ClickFraud).

Цели работы

- Разработка общей модели ботнетов и систем защиты от них
- Разработка стенда (системы) моделирования
- Решение практических задач в области защиты от ботнетов и атак DDoS

Релевантные работы (1/2)

- Проводимые исследования бот-сетей и методов противодействия им можно разделить на две категории.
- 1. Исследования, непосредственно посвященные разработке методов выявления бот-сетей и методов противодействия им;
- 2. Исследования, связанные с изучением бот-сетей, в частности с выявлением и спецификацией их функций, а также измерением параметров их функционирования.

Релевантные работы (2/2)

- Выявление бот-сетей может основываться на распознавании коллективных действий бот-узлов в сети Gu et al, 2008, определении сигнатур коммуникационного трафика, инициируемого ботами Binkley, Singh, 2006, и обнаружении соответствующих типов атак, проводимых бот-сетями Chen, Song, 2005, Mirkovic et al, 2004.
- Исследование параметров бот-сетей, позволяют лучшее понять работу бот-сети, а так же определить параметры конкретных типов бот-сетей Bailey et al, 2009. Примерами работ, посвященных изучению параметров и измерению бот сетей, являются работы Dagon et al, 2007, Gianvecchio et al, 2008, Grizzard et al, 2007.

Сущность и особенности задачи моделирования бот-сетей (1/3)

- Основой предлагаемого подхода к моделированию бот-сетей и механизмов защиты от их воздействия является агентно-ориентированное моделирование.
- Модели бот-сети и механизмов защиты от воздействия бот-сети, в настоящей работе, задаются в виде моделей противоборства команд атаки и команд защиты.
- Каждая команда представляет собой некоторое подмножество узлов вычислительной сети, определенных в виде соответствующих агентов, и имеющих общую коллективную цель.

Сущность и особенности задачи моделирования бот-сетей (2/3)

Команда атаки представляется агентами, входящими в состав бот-сети и реализующими действия, направленные на реализацию коллективной цели - обеспечение жизнедеятельности бот-сети.

Команда защиты формируется из агентов, выполняющих функции защиты и имеющих коллективную цель - противодействие процессу функционирования бот-сети.

Сущность и особенности задачи моделирования бот-сетей (3/3)

Основной парадигмой, используемой в данной работе, является представление узлов бот-сети в виде множества интеллектуальных автономных агентов.

Алгоритм поведения отдельного агента определяется его целевым назначением.

Агенты имеют возможность непосредственно выполнять свою целевую задачу и обмениваться информацией друг с другом, образуя команды, ориентированные на достижение одной общей цели.

Формальная модель (1/4)

Формальное представление *общей модели бот-сети и механизмов защиты* представлено в виде кортежа:

$$Q = <N, L, S, O>,$$ где

- N - узлы (хосты) вычислительной сети, L - связи между узлами вычислительной сети, S - сценарный компонент, O - компонент описывающий наблюдателя.

Формальная модель (2/4)

- Элементы множества N *узлов вычислительной сети* представляются в виде:

$$N = <T, R, P, F>, \text{ где}$$

- T - множество типов оборудования соответствующее узлу, R - множество функциональных ролей узла вычислительной сети, P - множество компонентов программного обеспечения, используемого узлами, $F : R \rightarrow P$ - функция, реализующая отображение множества функциональных ролей узла во множество компонент программного обеспечения.

Формальная модель (3/4)

- *Связи L между узлами вычислительной сети* в контексте различных протоколов описываются следующим образом. Будем считать, что узлы a,b связаны посредством протокола P_p' , если существует, хотя бы одна непустая конечная последовательность узлов с начальным узлом a и конечным b, через которые будет проходить сообщение $m_p \in E_p$, отправленное из узла a на узел b.
- Отдельный элемент множества L может быть записан в виде:

$$\forall l_{a,b}^{pp} \in L, \forall n_i \in N : R_{pp,j} = < n_a, ..., n_k, ..., n_b >, l_{a,b}^{pp} = < c_{pp,l}, R_{pp,1}, R_{pp,2}, ..., R_{pp,m} >,$$

- где $l_{a,b}^{pp}$ - соединение между узлами n_a и n_b посредством протокола *pp*, n_a и n_b - узлы вычислительной сети, $R_{pp,i}$ - i-й маршрут сообщения $m_p \in E_p$, $c_{pp,l}$ - дополнительные характеристики протокола .

Формальная модель (4/4)

Сценарный компонент $S =< S_B, S_D, S_N >$ включает в себя сценарии S_B функционирования бот-сети, сценарии S_D сдерживания бот-сети и противодействия атакам, а так же сценарии S_N легитимной деятельности вычислительной сети.

Каждый сценарий содержит следующие элементы:

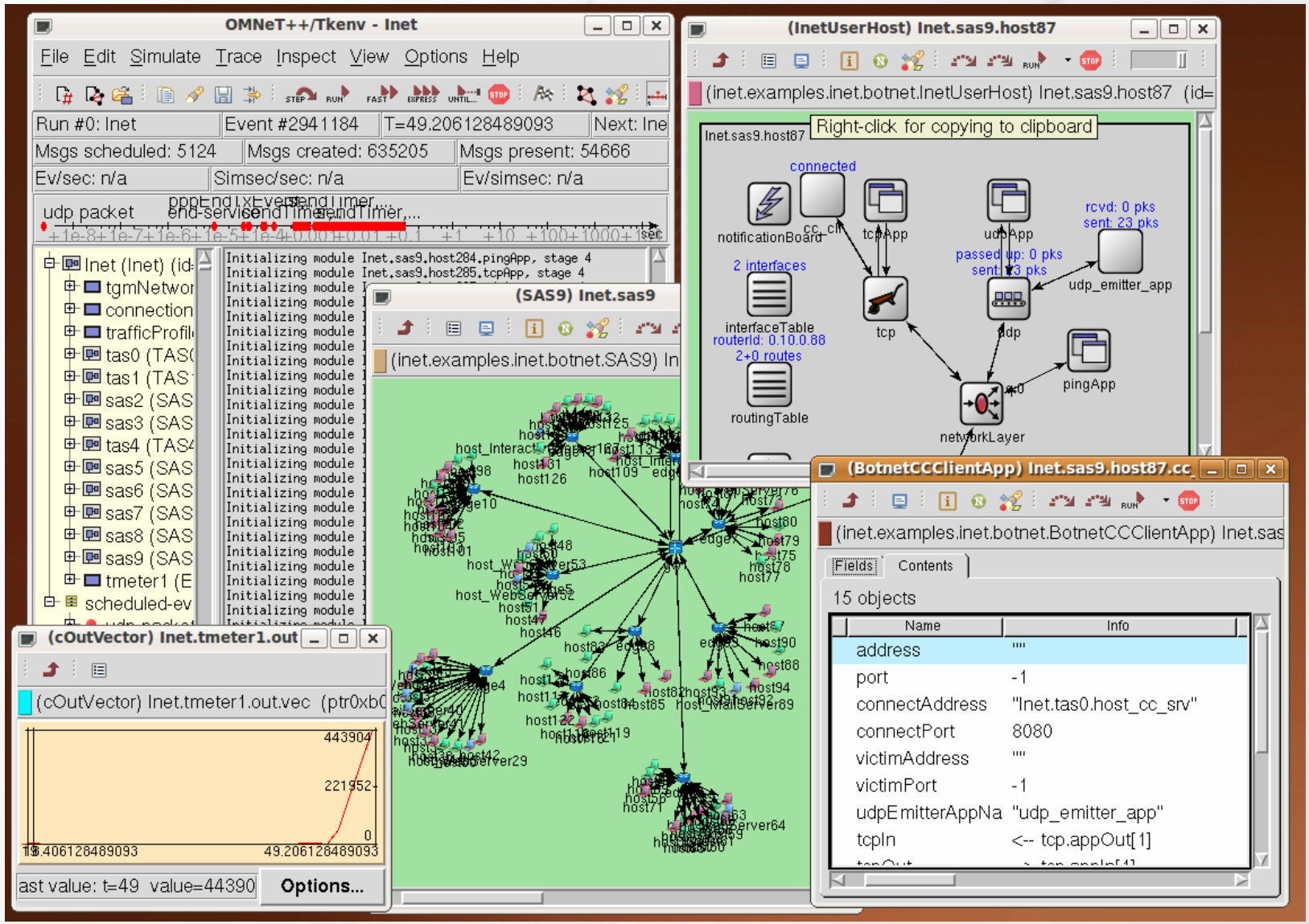
- цель сценария;
- алгоритм достижения цели;
- узлы, участвующие в сценарии; может иметь место разделение узлов на группы $H_i^j \subset N$, где i - номер группы, по исполняемым ролям или по иному признаку;
- множество включаемых в общий сценарий подсценариев

Архитектура среды моделирования

Система имитационного моделирования OMNeT++ (1/2)

- Система моделирования OMNeT++ представляет собой систему моделирования дискретных событий, и в предлагаемой модели является компонентом нижнего уровня.
- Система моделирования OMNeT++ обеспечивает процессы обмена сообщениями между компонентами модели, визуализацию хода эксперимента, взаимодействие модели с пользователем, а так же предоставляет отладчик моделей, позволяющий в наглядной форме отлеживать состояния объектов и последовательности модельных событий, что полезно при выявлении и устранении ошибок в процессе построения модели.

Система имитационного моделирования OMNeT++ (2/2)



Агенты бот-сети

Команда атаки представлена узлами следующих типов:

- узел “хозяин”
- узел “командный центр”
- узел “цель”
- узлы “зомби”.

- Узел “хозяин”, посредством рассылки команд, задаёт цели для бот-сети и контролирует поведение сети на самом высоком уровне.
- Узел “командный центр” осуществляет доставку команд полученных от “хозяина” к узлам “зомби”.
- Узлы “зомби”, получая команды от “командного центра”, непосредственно осуществляют действия согласно приказам “хозяина”.
- Узел “цель” выделяется из набора хостов, которые выполняют функции веб-сервера.

Агенты системы защиты (1/2)

Команда агентов защиты представлена узлами:

- первичной обработки информации (“сенсоры”)
- вторичной обработки информации (“сэмплеры”)
- обнаружения атаки (“детекторы”)
- фильтрации (“фильтры”)
- агенты ограничения трафика
- агенты “расследования”.

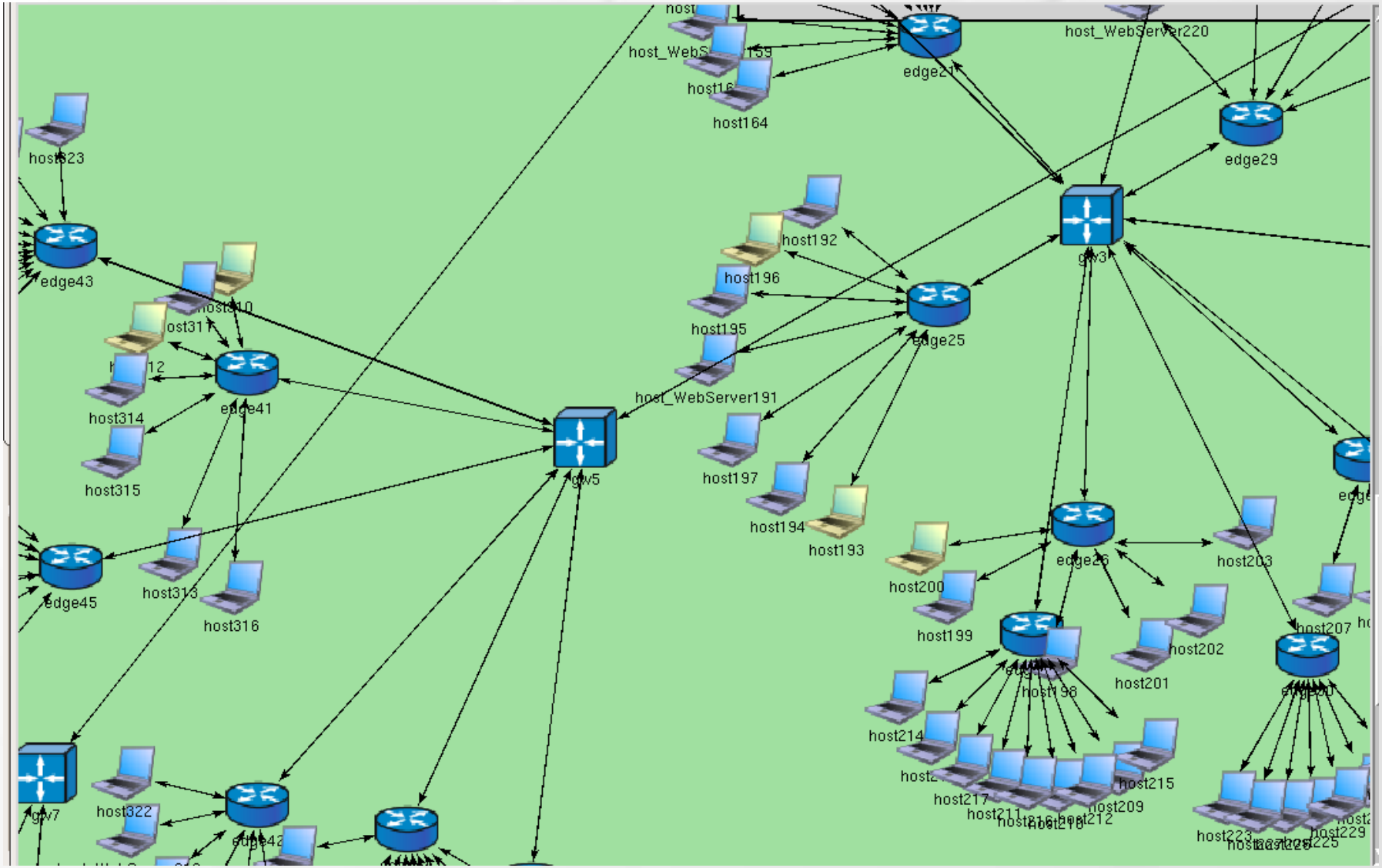
Агенты системы защиты (2/2)

- Сенсор обрабатывает информацию о сетевых пакетах и собирает статистические данные по трафику.
- Сэмплер, в режиме обучения, обрабатывает информацию о сетевых пакетах и составляет модель нормального трафика. В нормальном режиме, он анализирует сетевой трафик на соответствие модельному.
- Детектор на основе данных от сенсора и сэмплера принимает решение о наступлении атаки.
- Фильтр выполняет фильтрацию трафика на основе данных от детектора.
- Ограничитель предназначен для реализации кооперативной защиты от атак DDoS. Его задачей является ограничение трафика в соответствии с целью команды защиты
- Агент расследования – идентифицирует и выводит из строя агентов атаки.

Реализация сценариев (1/3)

- Для выполнения экспериментов были реализованы отдельные сценарии функционирования бот-сети (включая сценарии распространения бот-сети, управления бот-сетью и реализации атак), сценарии сдерживания бот-сети и противодействия атакам, а так же сценарии легитимной деятельности вычислительной сети.
- *Сценарии распространения бот-сети* включают сценарии поиска новых узлов, пригодных к компрометации, их идентификации и последующей компрометации и подключения инфицированных узлов в бот-сеть.
- Сценарий распространения бот-сети, использованный в экспериментах, основывается на модели распространения сетевого червя посредством эксплуатации уязвимости сетевых служб. После активации “уязвимого” сервиса, компьютер считается зараженным.

Реализация сценариев (2/3)



Реализация сценариев (3/3)

- *Сценарий управления* задается процедурой отправки сообщения о статусе нового узла на сервер “командный центр” с последующим ожиданием поступления команд со стороны сервера.
- Одним из примеров реализованных *сценариев атаки бот-сети* является атака вида UDP Flood, проводимая по отношению к некоторому узлу, IP-адрес которого указан в составе команды начала атаки.
- В настоящей работе реализовано несколько *сценариев сдерживания бот-сети и противодействия атакам*, направленных на защиту от атак DDoS: без кооперации; с кооперацией типа DefCOM; с кооперацией типа COSSACK и с полной кооперацией.

Сценарий защиты без кооперации

В *сценарии защиты без кооперации* используется только одна команда защиты. В этом случае команда может использовать следующие общие классы агентов:

- Сенсор;
- Сэмплер;
- Детектор;
- Фильтр;
- Расследования;
- Ограничитель.

Сценарий защиты на основе схемы DefCOM

- В соответствии со *сценарием защиты на основе схемы кооперации DefCOM ,* введены следующие классы агентов:
- Агент “Alert generator” основан на агенте “детектор”. Посредством данных, получаемых от агента “сэмплер”, он определяет множество IP-адресов узлов, которые генерируют наибольший трафик.
- Агент “Rate limiter” соответствует агенту “ограничитель”. Он отбрасывает сетевые пакеты, имеющие в качестве адреса назначения адрес узла – цели атаки.
- Агент “Classifier” базируется на агенте “фильтр”. Получая данные от агента “Alert generator”, выделяет и отбрасывает вредоносные пакеты, а так же отмечает легитимные пакеты, предписывая агенту “Rate limiter” не задерживать их.

Сценарий защиты на основе схемы COSSACK

- *Сценарий защиты на основе схемы кооперации COSSACK* включает класс агентов “snort”, который вычисляет статистические характеристики передаваемых пакетов для различных потоков трафика.
- Потоки группируются на основе префикса сетевого адреса. Когда трафик какого-либо потока превышает пороговое значение, его сигнатура передается агенту “watchdog”. Агент “watchdog” получает данные о трафике от агента “snort” и на их основе применяет правила фильтрации трафика на маршрутизаторах.
- Агент “фильтр” используется для моделирования выполнения фильтрации трафика на маршрутизаторе. Агент расположен на маршрутизаторе и для фильтрации трафика использует данные, получаемые от агента “watchdog”.

Сценарий полной кооперации

- *Сценарий полной кооперации* определяется следующими классами агентов защиты:
- Сенсор;
- Сэмплер;
- Детектор;
- Фильтр;
- Агент расследования.
- При данном сценарии агенты защиты атакуемой подсети могут свободно получать информацию от агентов защиты из других подсетей (других команд защиты) и управлять механизмами фильтрации на узлах других подсетей.

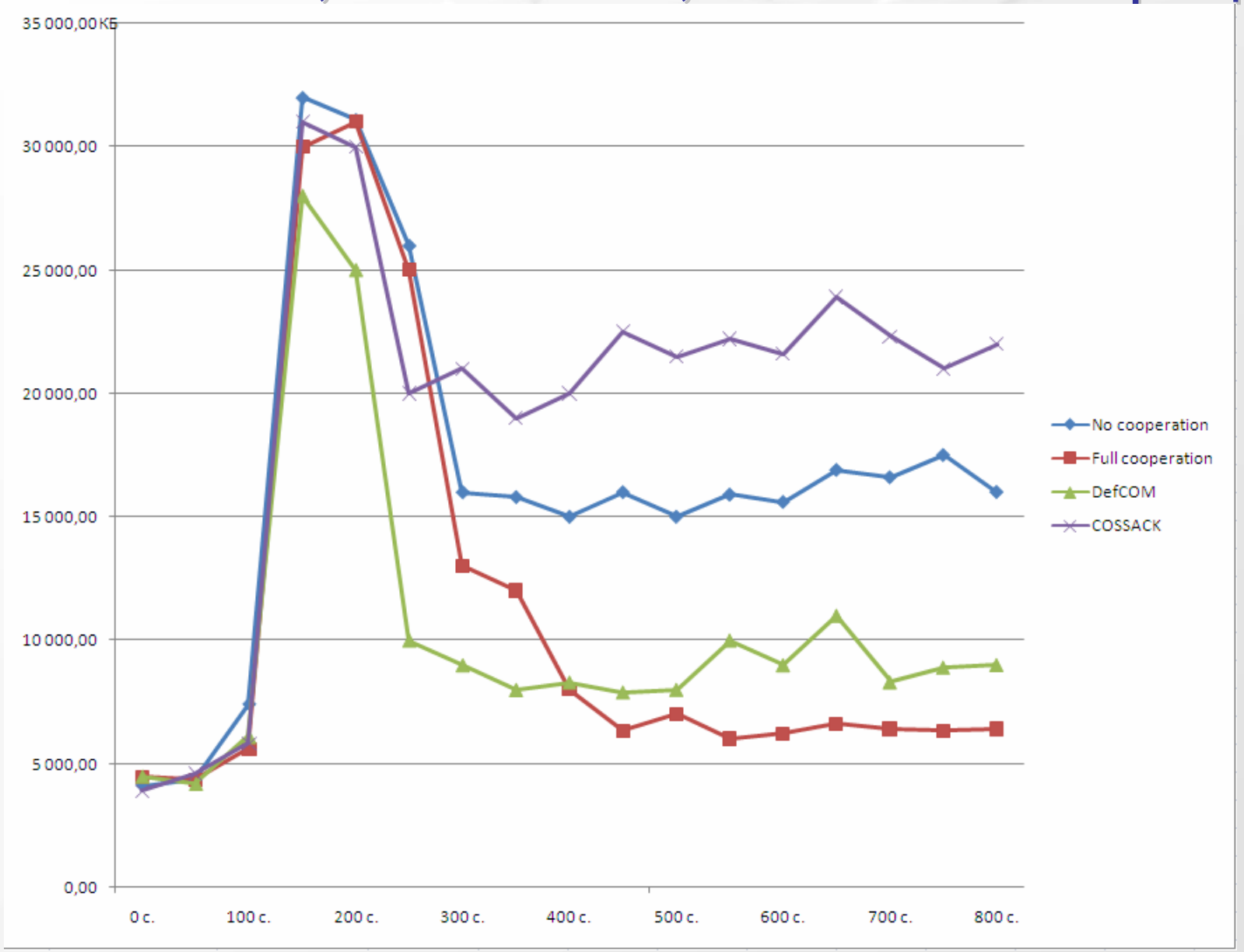
Сценарий легитимной деятельности сети

- Алгоритмы реализации *сценария легитимной деятельности вычислительной сети* основаны на генерации модельного трафика со статистическими параметрами, подобными параметрам трафика реальной сети.
- Они выполняются посредством подсценария создания сессии с использованием параметров, зависящих от типа генерируемого трафика.

Эксперименты

- Оценка результатов сценариев реализации атак и сценариев защиты проводилась по следующему классу параметров:
- количество входящих пакетов, принадлежащих атакующему трафику, до и после фильтрации, выполняемой командами, защищающими атакуемую сеть (узел);

Эксперименты. Без кооперации, DefCOM, COSSACK, полная кооперация



Заключение

- В настоящей работе предложен подход к исследовательскому моделированию бот-сетей и механизмов защиты от них в глобальной сети Интернет.
- Модели бот-сетей и методов защиты от них представлены в виде моделей противодействия команд интеллектуальных агентов, находящихся в отношениях кооперации или противодействия.
- Рассмотрены различные виды взаимодействия агентов, а так же на основе системы имитационного моделирования на базе дискретных событий (OMNET++) разработана программная среда для проведения экспериментов.

Дальнейшие исследования

- Дальнейшая работа посвящена:
- анализу эффективности функционирования различных команд атаки и защиты;
- исследованию различных типов внутрикомандного взаимодействия;
- реализации алгоритмов адаптации и самообучения команд защиты;
- разработке и исследованию новых способов защиты;
- расширению библиотеки агентов атаки и защиты.

Контактная информация

Коновалов Алексей Михайлович (ЗАО «Аркадия»)
alexonline@hotbox.ru
http://comsec.spb.ru/konovalov/

Шоров Андрей Владимирович (СПИИРАН)
ashorov@comsec.spb.ru
http://comsec.spb.ru/shorov/

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

Благодарности

Работа выполнена при финансовой поддержке РФФИ и программы фундаментальных исследований ОНИТ РАН.