МНОГОАГЕНТНОЕ МОДЕЛИРОВАНИЕ ДЛЯ ИССЛЕДОВАНИЯ МЕХАНИЗМОВ ЗАЩИТЫ ИНФОРМАЦИИ В СЕТИ ИНТЕРНЕТ

И. В. Котенко (Санкт-Петербург)

1. Введение

Одним из наиболее известных примеров больших открытых систем является среда Интернет, которая продолжает быстро развиваться. Любая компьютерная система, функционирующая в Интернет, должна быть способна взаимодействовать с различными компонентами, организациями и сетевыми операторами без постоянного управления со стороны пользователей. Такие функциональные возможности требуют возможности реализации динамического поведения, автономности и адаптации отдельных компонентов, использования методов, основанных на переговорах и кооперации, которые лежат в основе многоагентных систем [1].

Интернет постоянно находится под воздействием атак различных злоумышленников (как одиночек, так и организованных групп), зачастую достигающих своих целей. Злоумышленники-профессионалы для достижения своих целей способны реализовать развитые стратегии осуществления различных угроз безопасности. Поэтому обеспечение безопасности систем, функционирующих в Интернет, требует выполнения в реальном времени непрерывного комплекса разнообразных действий: реализация механизмов защиты, соответствующих установленной политике безопасности; сбор и анализ необходимой информации; обнаружение аномальной активности, нелегитимных действий, атак и вторжений; предсказание намерений и возможных действий злоумышленников; непосредственное реагирование на вторжения; рефлексивное управление поведением злоумышленника, усиление критических механизмов защиты; устранение последствий вторжения, выявленных уязвимостей и адаптация системы обеспечения информационной безопасности к последующим вторжениям.

Вопросы моделирования обеспечения информационной безопасности активно исследуются на протяжении более чем тридцати лет. Разработано большое количество разнообразных формальных и неформальных моделей отдельных механизмов защиты, но практически отсутствуют работы, формализующие комплексный антагонистический характер обеспечения информационной безопасности как сложного организационно-технического процесса. Это объясняется сложностью данной предметной области. Хотя исследователи в состоянии представить отдельные механизмы защиты, понимание системы обеспечения информационной безопасности как единой системы, зависящей от учета множества взаимодействий между отдельными процессами и развивающегося динамического характера этих процессов и отдельных компонент информационных систем, чрезвычайно затруднено. Особенно это справедливо с учетом наблюдаемой в настоящее время эволюции Интернет в свободную децентрализованную распределенную среду взаимодействия огромного числа кооперирующихся и антагонистических программных агентов [1–3].

В настоящей работе данная проблема рассматривается на примере исследования и реализации механизмов защиты от распределенных сетевых атак. Одним из наиболее критичных представителей этих атак является “распределенный отказ в обслуживании” (Distributed Denial of Service, DDoS). Для проведения данного класса атак злоумышленник должен сначала скомпрометировать огромное число компьютеров, а затем организовать последующее совместное нападение на некоторый сетевой ресурс. Построение системы защиты от таких атак является сложной задачей. Эффективная система защиты должна включать механизмы предупреждения атаки, обнаружения факта атаки, определения источника атаки и противодействия атаке.

Разработать адекватные методы защиты и выработать обоснованные рекомендации по выбору механизмов защиты, наиболее действенных в конкретных условиях, можно, используя *исследовательское моделирование* атак и механизмов защиты от них. Формализация, моделирование и исследование противоборства злоумышленников и систем защиты в компьютерных сетях на примере моделирования процессов реализации распределенных атак и механизмов защиты от них может позволить получить результаты, обобщаемые на другие задачи, в частности, на задачи информационной борьбы, конкуренции в сфере электронного бизнеса и др.

В работе развивается подход к исследованию противоборства в компьютерных сетях на основе моделирования антагонистического взаимодействия команд агентов, представляющих злоумышленников и компоненты систем защиты, предложенный в [2–3]. Работа структурирована следующим образом. Во *втором разделе* излагается сущность подхода к моделированию. В *третьем разделе* описывается архитектура и реализация используемой среды многоагентного моделирования. В *четвертом разделе* характеризуются проведенные эксперименты. В *заключении* формулируются результаты работы и направления будущих исследований.

2. Особенности предлагаемого подхода

Основу для исследования составляет теория командной работы агентов. Еще одной фундаментальной составляющей проводимых исследований являются работы в области систем вывода, основанных на знаниях о выполняемых действиях и предсказании намерений и планов оппонента на основе оценки текущей ситуации. Важной компонентой, необходимой для использования в работе, являются методы теории рефлексивных процессов, теоретико-игрового информационного моделирования и управления в конфликтных ситуациях. Команды агентов атаки и защиты должны адаптироваться к реконфигурации аппаратного и программного обеспечения сети, к изменению трафика, а также к новым видам защиты и атакам на основе прошлого опыта и алгоритмов. Поэтому важно учитывать существующие исследования в области адаптации и самообучения агентов.

Предлагаемый в настоящей работе подход к организации командной работы агентов базируется на совместном использовании элементов теории общих намерений, теории разделяемых планов и комбинированных подходов [4, 5] и учитывает технологии реализации многоагентных систем и многоагентного моделирования [6].

Использование основанного на многоагентных технологиях моделирования процессов обеспечения безопасности Интернет предполагает, что кибернетическое противоборство представляется в виде взаимодействия команд программных агентов [2, 3]. Агрегированное поведение системы проявляется через локальные взаимодействия агентов в динамической среде, задаваемой посредством модели сети.

Абстрактная модель взаимодействия команд агентов в среде Интернет включает следующие компоненты (рис. 1) [2]: онтологию приложения, содержащую множество понятий приложения и отношений между ними; протоколы командной работы агентов различных команд; модели сценарного общекомандного, группового и индивидуального поведения агентов; библиотеки базовых функций агентов; коммуникационную платформу и компоненты, предназначенные для обмена сообщениями между агентами; модели среды функционирования – компьютерной сети, включающие топологический и функциональные компоненты.

Выделяется две команды агентов, воздействующих на компьютерную сеть, а также друг на друга: команда агентов-злоумышленников по реализации атак и команда агентов защиты. Задача многоагентного моделирования представляется как моделиро-

вание антагонистического взаимодействия, по крайней мере, одной команды агентов-злоумышленников и одной команды агентов защиты.

Агенты различных команд соперничают для достижения противоположных намерений. Агенты одной команды сотрудничают для осуществления общего намерения (по реализации угрозы или по защите компьютерной сети). Выбор сценария поведения каждой из команд зависит, прежде всего, от выбранной цели функционирования, а конкретная реализация сценария определяется, в первую очередь, непосредственной реакцией противоположной команды. Выбор очередного шага поведения каждой из команд должен определяться динамически в зависимости от действий противоположной команды и состояния среды.

Каждая команда действует в условиях ограниченной информации, а каждый член команды может обладать различной информацией о действиях других членов команды. Поэтому модель поведения агентов должна быть в состоянии отображать неполноту информации и возможность возникновения случайных факторов. Кроме того, само поведение агентов должно зависеть от информации, которой владеет команда, и от ее распределения на множестве агентов, входящих в состав команды [2].

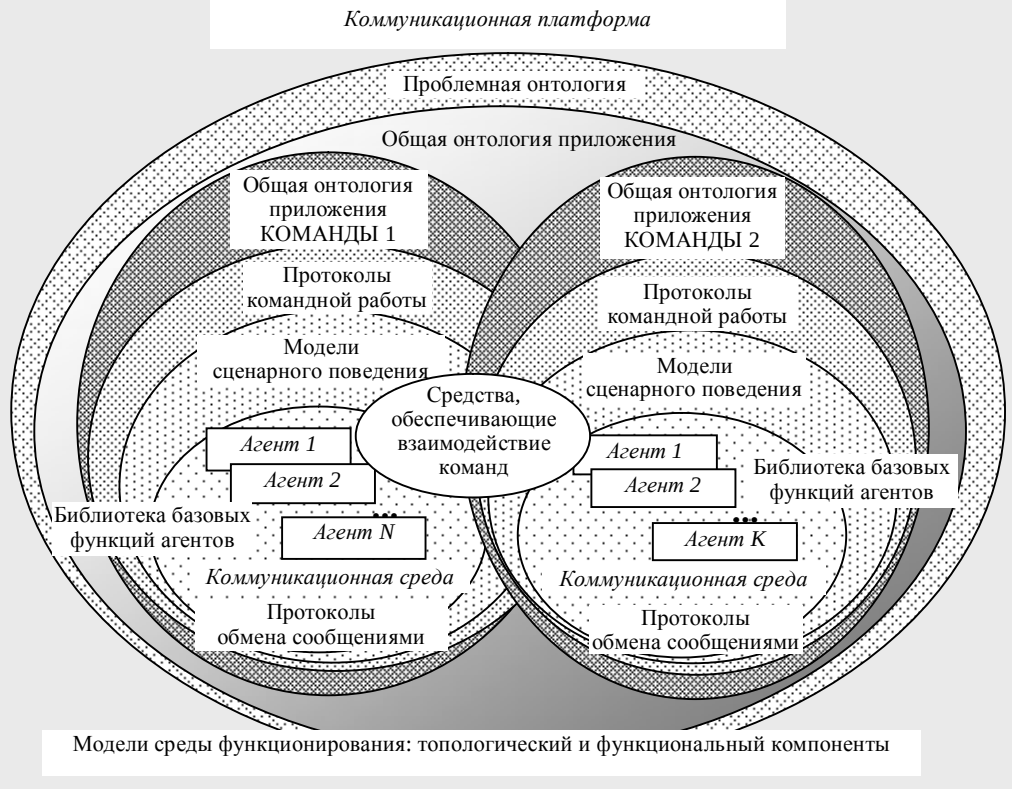

Рис. 1. Абстрактная модель взаимодействия команд агентов в среде Интернет

Модели функционирования агентов должны предусматривать, что каждый агент “знает”, какие задачи он должен решать сам и к какому агенту он должен адресовать свой запрос на информацию или на решение подзадачи с целью получения такой информации, если это вне его компетенции. Сообщения одних агентов представляются в форме и терминах, понятных другим агентам. Специализация каждого агента отражается подмножеством узлов онтологии. Некоторые узлы онтологии могут быть общими для пары или большего количества агентов. Обычно только один из этих агентов обладает детально структурированным описанием этого узла. Именно этот агент является

обладателем соответствующего фрагмента базы знаний. В то же время, некоторая часть онтологических баз знаний является общей для всех агентов и играет роль общего контекста (общих знаний).

В работе используется следующая структура и функциональность команд атаки и защиты. *Агенты атаки* подразделяются, по крайней мере, на два класса: “демоны”, непосредственно реализующие атаку, и “мастер”, выполняющий действия по координации остальных компонентов системы. Выделены следующие классы *агентов защиты*: обработки информации (“сэмплеры”), обнаружения атаки (“детекторы”); фильтрации и балансировки нагрузки (“фильтры”); расследования и деактивации агентов атак (“агенты расследования”).

Механизмы взаимодействия и координации агентов базируются на трех группах процедур: обеспечение согласованности действий; мониторинг и восстановление функциональности агентов; обеспечение селективности коммуникаций.

Процедуры обеспечения согласованности действий агентов необходимы для поддержки скоординированной деятельности агентов по некоторому сценарию. Эти процедуры реализуются путем обмена агентами информацией о результатах деятельности, которые непосредственно влияют на выполнение поставленной задачи. До начала реализации распределенной атаки происходит формирование необходимого количества агентов, до их сведения доводятся их роли. Далее агенты сообщают о своей готовности и начинают активные действия в соответствии с заданной ролью. При достижении поставленной цели, обнаружении невозможности выполнить цель или выявлении нерелевантности цели агент обязан сообщить этот факт оставшимся членам команды. При этих условиях выполняемый сценарий завершается и должен быть активизирован другой сценарий.

Процедуры мониторинга и восстановления функциональности агентов направлены на сохранение работоспособности и функциональности команды агентов. Их реализация может происходить с использованием различных приемов, например, за счет перераспределения ролей среди оставшихся агентов взамен выбывших или путем генерации новых агентов с соответствующей ролью и функциональностью, если количество работоспособных агентов достигло критического числа.

Процедуры обеспечения селективности коммуникаций служат для минимизации количества коммуникативных актов с целью уменьшения вероятности раскрытия агентов и сокращения используемых ресурсов. Эти процедуры реализуются на основании знаний о выгоде коммуникационного акта и “затратах” на его обеспечение.

Предполагается, что агенты могут реализовать *механизмы самоадаптации* и *эволюционировать* в процессе функционирования. 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 механизмов и профилей защиты.

Для исследовательского моделирования предлагается использовать семейство различных моделей (от аналитических до полунатурных и натурных) (рис. 2) [7].

Выбор конкретных моделей диктуется необходимой точностью и масштабируемостью моделирования. Например, аналитические модели позволяют имитировать глобальные процессы, происходящие в компьютерных сетях, однако эти модели описывают моделируемые процессы только на абстрактном уровне. Имитационное моделирование на уровне пакетов предоставляет возможность достаточно адекватно воспроизводить протекающие процессы, представляя атакующие и защитные действия с помощью обмена сетевыми пакетами, точно имитируя работу по протоколам канального, сетевого, транспортного и прикладного уровней. Наибольшая точность имитации до-

стигается на аппаратных стендах при натурном моделировании, однако при этом удается моделировать достаточно ограниченные фрагменты взаимодействий агентов. Основное внимание в настоящей работе уделяется применению имитационного моделирования на уровне пакетов с использованием средств имитации сетевых процессов в качестве базового уровня среды моделирования.

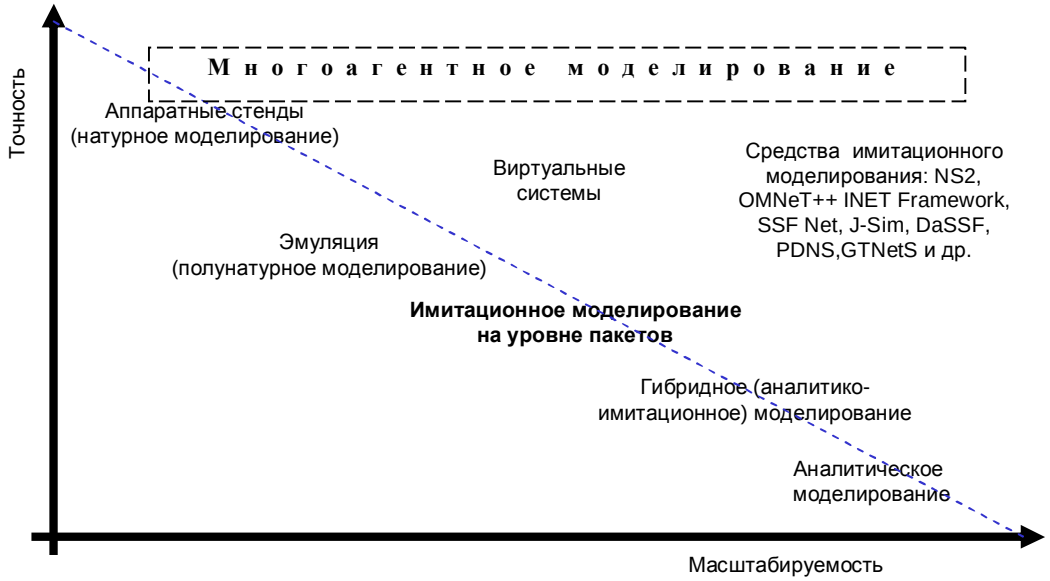

Рис. 2. Семейство моделей, используемых для исследовательского моделирования компьютерного противоборства

3. Среда моделирования

Для реализации представленного подхода к моделированию механизмов защиты разработана многоуровневая программная система, отличающаяся от известных средств агентно-ориентированного моделирования (например, CORMAS, Repast, Swarm, MadKit, MASON, NetLogo и др.) [6], в первую очередь, использованием в качестве базиса средств (пакетов) имитационного моделирования, позволяющих адекватно имитировать сетевые процессы. Поэтому для реализации подхода используется архитектура системы моделирования (рис.3), включающая базовую систему имитационного моделирования (Simulation Framework), модуль (пакет) моделирования сети Интернет (Internet Simulation Framework), подсистему многоагентного моделирования (Agent-based Framework) и модуль (библиотеку) имитации процессов предметной области (Subject Domain Library).

Компонент Simulation Framework представляет собой систему моделирования на основе дискретных событий. Остальные компоненты являются надстройками или моделями для Simulation Framework.

Компонент Internet Simulation Framework – комплект модулей, позволяющих реалистично моделировать узлы и протоколы сети Интернет. Сеть состоит из узлов, узел содержит стек IP протоколов. Дополнительно можно подключать модули, реализующие протоколы транспортного уровня.

Многоагентное моделирование реализуется посредством *компонента Agent-based Framework*, который использует модуль имитации процессов предметной области. Данный компонент представляет собой библиотеку модулей, задающих интеллектуальных агентов, реализованных в виде приложений. При проектировании и реализации модулей агентов подразумевается использование элементов абстрактной архитек-

туры FIPA [8]. Для взаимодействия агентов необходим язык коммуникаций. Передача сообщений между ними происходит поверх TCP-протокола, реализованного в компоненте Internet Simulation Framework. Каталог агентов является обязательным только для агента, координирующего действия других. Агенты могут управлять другими модулями с помощью сообщений.

Рис. 3. Архитектура системы моделирования

Компонент Subject Domain Library – это библиотека, служащая для имитации процессов предметной области, а также модули, дополняющие функциональность IP-узла: таблица фильтрации и анализатор пакетов.

Так как все моделируемые процессы происходят в Интернет, то в основе системы моделирования должна быть модель этой сети. Для выбора инструментария моделирования сети и процессов передачи информации был проведен анализ различных пакетов моделирования сетей, включая NS2, OMNeT++ INET Framework, SSF Net, J-Sim INET Framework и ряда других. В качестве основных требований, которые предъявлялись к используемому инструментарию моделирования, были выбраны следующие: детальная реализация протоколов, которые задействованы в атаках, начиная от сетевого уровня, чтобы была возможность моделирования известных атак; возможность написания и подключения собственных модулей для реализации агентского подхода; возможность изменения параметров моделирования во время симуляции; реализация для Windows или Linux (либо независимость платформы); развитый графический интерфейс; бесплатность при использовании в исследовательских целях.

Проведенный анализ показал, что этим требованиям в наилучшей степени удовлетворяет OMNeT++ INET Framework [9], являющийся пакетом для OMNeT++. С использованием OMNeT++ INET Framework и программных моделей, разработанных на C++, представленная выше архитектура была реализована для многоагентного модели-

рования атак DDoS и механизмов защиты от них. Модели агентов, реализованные в Agent-based Framework, представлены типовым агентом, агентами атаки и агентами защиты. Subject Domain Library содержит различные модели узлов, например, атакующего, брандмауэра и др., а также модели приложений (механизмы реализации атак и защиты, анализаторы пакетов, таблицы фильтрации).

Система OMNeT++ представляет собой инструментарий моделирования дискретных событий, написанный на языке C++ и предназначенный, в первую очередь, для моделирования компьютерных сетей и других распределенных систем. Принцип работы OMNeT++ заключается в следующем. Изменение состояния моделируемой системы происходит в дискретные моменты времени по списку будущих событий (future event list), отсортированных по времени. Событием может быть: начало передачи пакета, тайм-аут и т.п. События происходят на основе выполнения простых модулей (simple module). У такого модуля есть функции инициализации, обработки сообщения, действия и завершения работы. Обмен сообщениями между модулями осуществляется по каналам (channel), с которыми соединены модули своими шлюзами (gate), или непосредственно через шлюзы. Шлюз может быть входящим и исходящим, соответственно для приема и посылки сообщений.

Система INET Framework – это комплект модулей с открытым исходным кодом, позволяющих реалистично моделировать узлы и протоколы проводных и беспроводных сетей. Он включает модели различных протоколов Интернета: IP, IPv6, TCP, UDP, 802.11, Ethernet, PPP, MPLS с LDP и RSVP-TE signalling, OSPF и ряд других. В комплект также входят различные реалистичные примеры использования этих протоколов.

Наивысший уровень абстракции в моделировании IP в INET Framework – это сеть, состоящая из IP-узлов. Узел может быть маршрутизатором или хостом. IP-узел отвечает компьютерному представлению стека протоколов Интернет. Модули, из которых он состоит, организованы так, как происходит обработка IP-дейтаграммы в операционных системах. Обязательным является модуль, отвечающий за сетевой уровень (реализующий обработку IP) и модуль “сетевой интерфейс”. Дополнительно подключаются модули, реализующие протоколы транспортного уровня.

В реализованной системе моделирования OMNeT++ INET Framework подверглась множеству различных модификаций. В том числе были созданы таблица фильтрации пакетов на сетевом уровне для моделирования действий агентов защиты и модуль, позволяющий просматривать весь трафик данного узла для ведения статистики, а также для моделирования действий агентов защиты. Подверглись изменению модули, отвечающие за работу «Sockets» для моделирования атак и механизмов защиты.

Реализована система многоагентного моделирования Multiagent Framework. Агенты атаки и защиты были реализованы в виде сложных модулей (compound module). Они содержат простые модули, отвечающие за работу по различным сетевым протоколам, и ядро агента. Ядро агента служит для управления остальными модулями. Агент, как сложный модуль, имеет ряд шлюзов для подключения к стандартному сетевому узлу из INET Framework. Эти шлюзы относятся к соответствующим сетевым протоколам. Подключение или установка агента может происходить во время проведения моделирования.

Ядра агентов выполнены на основе сопрограмм, так как это удобно для реализации протоколов взаимодействия, положенных в основу командной работы агентов. Остальные модули реализованы как обработчики сообщений от ядра и внешней среды.

В библиотеке предметной области содержатся модели атак и защиты. Модели реализованы в виде параметризуемых модулей, которые устанавливаются как приложения на узлы сети, а также включаются в состав агентов. Для этого реализованы протоколы взаимодействия между ядром агента и модулем атаки или защиты.

Пример многооконного пользовательского интерфейса среды моделирования показан на рис.4. На основном окне визуализации (рис.4, вверху справа) отображается компьютерная сеть для проведения моделирования. Окно управления процессом моделирования (рис.4, внизу справа) позволяет просматривать и менять параметры моделирования. В данном окне на шкале времени можно наблюдать события, значимые для понимания атак и механизмов защиты. Шкала времени отображается над окном с текстовым описанием событий. Для отображения текущего состояния команд агентов служат соответствующие окна состояний (рис.4, сверху посередине). Можно открывать различные окна, характеризующие функционирование (статистические данные) отдельных хостов, протоколов и агентов, например, на рис.4 (слева) отображено несколько окон, характеризующих в графическом и текстовом виде (в том числе в форме графика зависимости количества переданных бит от времени) функционирование одного из хостов.

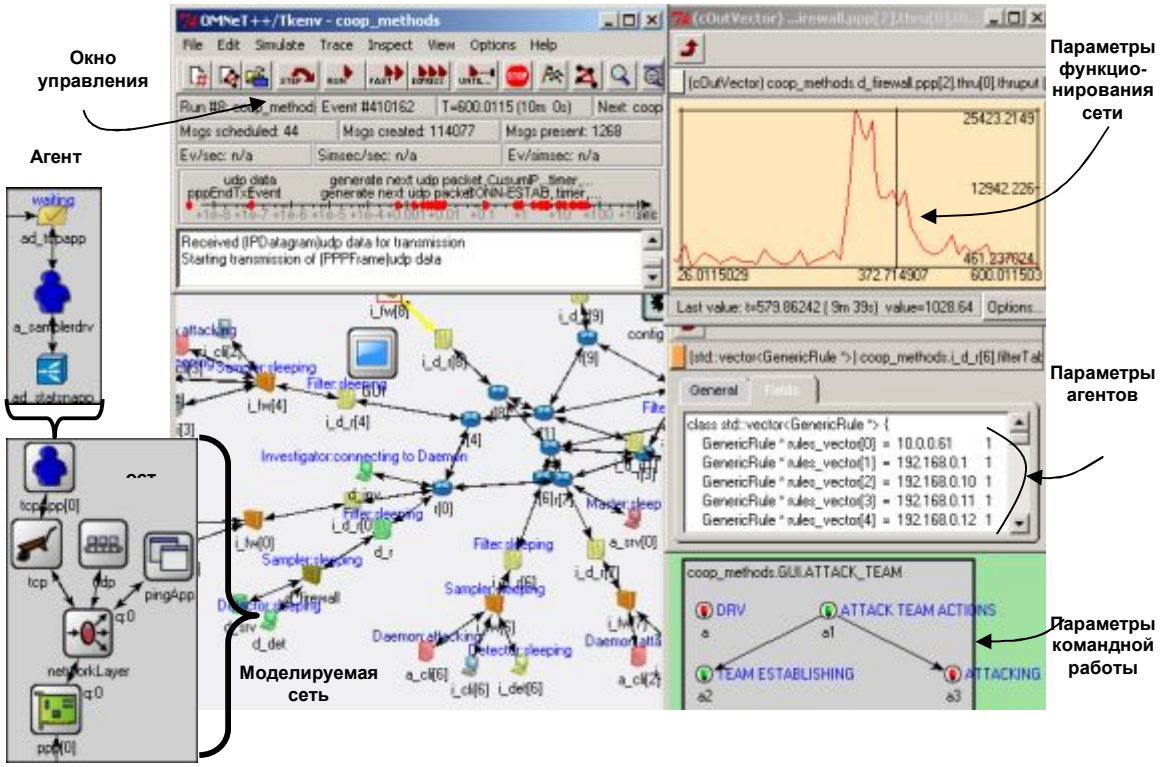

Рис. 4. Пользовательский интерфейс среды моделирования

4. Эксперименты

Созданная система моделирования позволяет проводить различные эксперименты с целью исследования стратегий реализации атак и механизмов защиты от них. В процессе использования системы моделирования можно варьировать топологию и конфигурацию сети, структуру и конфигурацию команд атаки и защиты, механизмы реализации атак и защиты, параметры кооперации команд и другие. Задавая различные адаптивные стратегии действий команд, можно наблюдать за процессом выполнения командами агентов своих функций и эволюции их поведения и изменения состояния глобальной сети. На основе экспериментов проводятся измерения различных показателей эффективности механизмов защиты и выполняется анализ условий и возможности их применения.

Проведено представительное число экспериментов по исследованию как известных, так и предложенных авторами механизмов защиты от распределенных атак. В том числе анализировались различные кооперативные схемы защиты и схемы адаптации. Проведены эксперименты по изучению таких известных кооперативных механизмов защиты, как DefCOM [10] и COSSACK [11]. Проанализированы также предложенные кооперативные механизмы защиты (с кооперацией на уровне фильтров, с кооперацией на уровне сэмплеров, со слабой и полной кооперацией).

Исследована, например, следующая адаптивная схема взаимодействия команд. Команда атаки начинала атаку в некоторый момент времени с определенными интенсивностью и методом подмены адреса отправителя. Во время атаки, если мастер обнаруживал, что какой-то из демонов неработоспособен, он изменял параметры атаки, чтобы сохранить интенсивность и предотвратить обнаружение. Команда защиты изначально работала, используя наименее ресурсоемкий способ защиты. Как только обнаруживалась атака, делалась попытка заблокировать пакеты от атакующих, проследить их и обезвредить. Если это не удавалось, метод защиты заменялся на другой, более сложный. Для эксперимента использовались кооперативные схемы команд “на уровне фильтров”, “на уровне сэмплеров” и “полная кооперация”.

Заключение

В статье рассмотрен предлагаемый подход к многоагентному моделированию процессов защиты информации. Подход представлен на примере антагонистического противоборства двух команд агентов: агентов реализации атак и агентов защиты от данного класса атак. Рассмотрены особенности подхода, описана разработанная среда моделирования и представлены некоторые из сценариев моделирования.

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 защиты ведет к существенному повышению ее эффективности.

Направления дальнейших работ связаны с исследованием механизмов защиты от различных типов атак, а также с совершенствованием системы моделирования. Работа выполнена при финансовой поддержке РФФИ (проект №07-01-00547) и программы фундаментальных исследований ОНИТ РАН (контракт №3.2/03). Автор выражает благодарность разработчикам программной среды моделирования и отдельных приложений – Уланову А.В., Коновалову А.М., Шорову А.В. и др.

Литература

1. **Городецкий В. И., Котенко И. В.** Командная работа агентов-хакеров: применение многоагентной технологии для моделирования распределенных атак на компьютерные сети // КИИ-2002. VIII Национальная конференция по искусственному интеллекту с международным участием. Труды конференции. М.: Физматлит, 2002.
2. **Городецкий В. И., Котенко И. В.** Концептуальные основы стохастического моделирования в среде Интернет // Труды института системного анализа РАН. Т. 9: Фундаментальные основы информационных технологий и систем. Под ред. С.В.Емельянова. М.: URSS, 2005.
3. **Котенко И. В., Уланов А. В.** Агентно-ориентированное моделирование поведения сложных систем в среде Интернет // КИИ-2006. X Национальная конференция по искусственному интеллекту с международным участием. Труды конференции. Т. 2. М.: Физматлит, 2006. С. 660–668.

4. **Котенко И. В., Станкевич Л. А.** Командная работа агентов в реальном времени // Новости искусственного интеллекта, № 3, 2003. С. 25–31.
5. **Kaminka G. A., Yakir A., Erusalimchik D., Cohen N.** Towards Collaborative Task and Team Maintenance // Proceedings of the Sixth International Joint Conference on Autonomous Agents and Multi-Agent Systems (AAMAS-07), 2007.
6. **Macal C. M., North M. J.** Agent-based Modeling and Simulation: ABMS Examples // Proceedings of the 2008 Winter Simulation Conference. 2008.
7. **Perumalla K. S., Sundaragopalan S**. High-Fidelity Modeling of Computer Network Worms // Technical Report GIT-CERCS-04-23. Center for Experimental Research in Computer Science. Georgia Institute of Technology. 2004.
8. FIPA. http://www.fipa.org
9. OMNeT++ homepage. http://www.omnetpp.org/
10. **Mirkovic J., Robinson M., Reiher P., Oikonomou G.** Distributed Defense against DDOS Attacks // University of Delaware CIS Department Technical Report CIS-TR-2005-02, 2005.
11. **Papadopoulos C., Lindell R., Mehringer I., Hussain A., Govindan R.** Cossack: Coordinated suppression of simultaneous attacks // Proceedings of DISCEX III, 2003.