УДК 681.3.053:681.32:007.5

КООПЕРАТИВНАЯ РАБОТА КОМАНД АГЕНТОВ ПРИ ЗАЩИТЕ ОТ СЕТЕВЫХ АТАК НАРУШЕНИЯ ДОСТУПНОСТИ*

И.В.Котенко[1], А.В. Уланов[2]

В работе предлагается подход к созданию кооперативной многоагентной системы защиты от распределенных атак, направленных на нарушение доступности. Подход основан на представлении нарушителей и систем защиты в виде команд взаимодействующих агентов. Авторами предлагается система агентно-ориентированного моделирования для проверки эффективности разработанных моделей. Приводятся результаты различных экспериментов. Анализируются различные параметры кооперативной работы команд агентов и их влияние на эффективность защиты.

Введение

Одной из актуальных текущих угроз безопасности Интернет являются *атаки "распределенный отказ в обслуживании"* (Distributed Denial of Service, DDoS). Реализация этих атак может привести не только к выходу из строя отдельных хостов и служб, но и остановить работу корневых DNS-серверов и вызвать частичное или полное прекращение функционирования Интернета. Для проведения данной атаки нарушители должны сначала скомпрометировать большое количество хостов, установить на них агентов атаки, а затем осуществить последующее одновременное нападение на хосты или целые подсети Интернет. Атаки осуществляются с помощью посылки жертве большого количества сетевых пакетов, передачи слишком длинных пакетов, некорректных пакетов или большого количества трудоемких запросов и др.

* Работа выполнена при финансовой поддержке РФФИ (проект № 04-01-00167), программы фундаментальных исследований ОИТВС РАН (контракт № 3.2/03), Фонда содействия отечественной науке и при частичной финансовой поддержке, осуществляемой в рамках проекта Евросоюза POSITIF (IST-2002-002314).

[1] *199178, С.-Петербург, 14 линия, 39, СПИИРАН, ivkote@iias.spb.su*

[2] *199178, С.-Петербург, 14 линия, 39, СПИИРАН, ulanov@iias.spb.su*

Эффективная защита от атак DDoS должна строиться на основе распределенной многокомпонентной системы, и включать механизмы предупреждения и обнаружения атаки, определения ее источников и противодействия. Очевидно, что чем большим количеством информации обладает система защиты, тем точнее можно обнаружить атаку. Однако из-за отсутствия в сети Интернет единого управления в большинстве случаев невозможно получить данные о трафике во всех указанных подсетях. Наиболее вероятная ситуация – сбор данных в промежуточной и (или) защищаемой сети, например, от своего поставщика услуг Интернет (ISP).

Актуальной задачей, требующей решения для создания интеллектуальных информационно-безопасных распределенных вычислительных систем, является задача формализации противодействия нарушителей и систем защиты в сети Интернет и, в частности, исследования атак DDoS и разработки эффективных средств защиты от них. В работе рассматривается развитие изложенного в [Котенко и др., 2005; Kotenko et al., 2005] подхода к многоагентному моделированию атак DDoS и защиты от них для исследования безопасности Интернет. Используя разработанную среду моделирования, авторы исследуют различные способы противодействия атакам DDoS, представляя компоненты атаки и защиты в виде команд агентов. В том числе в работе допускается *возможность кооперации между различными командами агентов защиты как компонентами систем защиты различных поставщиков услуг Интернет*. В *первом разделе* кратко характеризуются основы предлагаемого подхода, и дается описание моделей команд агентов, реализующих атаки DDoS и защиту. Во *втором разделе* представлена разработанная среда моделирования. В *третьем разделе* описываются проведенные эксперименты. В *заключении* формулируются результаты работы и направление будущих исследований.

1. Подход к моделированию

Использование основанного на многоагентных технологиях моделирования процессов поведения сложных систем в сети Интернет предполагает, что формализуемые процессы представляются в виде взаимодействия различных команд программных агентов в динамической среде, задаваемой на основе модели сети Интернет [Kotenko et al., 2005]. Агрегированное поведение системы проявляется посредством локальных взаимодействий отдельных агентов. Предполагается, что агенты осуществляют сбор информации из различных источников, оперируют нечеткими знаниями, прогнозируют намерения и действия других агентов,

оценивают возможные риски, пытаются обмануть агентов соперничающих команд, реагируют на действия других агентов.

При формализации данной задачи выделяются различные классы команд агентов: агенты-злоумышленники, агенты защиты и агенты-пользователи. Агенты различных команд могут находиться в отношении безразличия, сотрудничать или соперничать, вплоть до явного противоборства. Предлагаемый подход к организации командной работы агентов базируется на совместном использовании элементов теории общих намерений, теории разделяемых планов и комбинированных подходов, а также учитывает опыт программной реализации многоагентных систем GRATE, OAA, CAST, RETSINA-MAS, COGNET/BATON и др.

Агенты команд атаки подразделяются, по крайней мере, на два класса: “демоны”, реализующие атаку, и “мастер”, выполняющий действия по координации остальных компонентов системы. На предварительном этапе демоны и мастер устанавливаются на доступные узлы сети. Класс атаки задается следующим набором параметров: интенсивностью посылки пакетов и способом подмены адреса отправителя в пакете (“IP spoofing”): без подмены, постоянный, случайный, случайный с реальными адресами.

В соответствии с общим подходом к защите от DDoS атак, выделены следующие классы *агентов команд защиты*: обработки информации (“сэмплеры”), обнаружения атаки (“детекторы”); фильтрации (“фильтры”); “агенты расследования”. Сэмплеры осуществляют сбор сетевых данных для последующего обнаружения аномалий или злоупотреблений детектором. Фильтры ответственны за фильтрацию трафика атаки по правилам, предоставляемым детектором. Агент расследования пытается обезвредить агентов атаки. Команда агентов защиты совместно реализует определенный исследуемый механизм защиты. Команды агентов защиты могут *взаимодействовать по различным схемам*. В одной из них при обнаружении начала атаки действует детектор команды, на защищаемую сеть которой направлена атака (сети-жертвы). Он посылает запрос агентам-сэмплерам других команд с целью получения информации, которая может быть релевантной указанной атаке. Сэмплеры других команд отвечают на запрос, посылая необходимые данные. Эта информация существенно повышает шансы на обнаружение атаки. В случае обнаружения вероятного источника атаки детектор сети-жертвы посылает информацию об адресе агента атаки детектору команды, в сети которой может находиться этот агент, с целью его деактивации.

2. Среда моделирования

При разработке среды моделирования были проанализированы существующие системы многоагентного моделирования: Swarm, Java Swarm, Repast, MASON, NetLogo и др. Swarm предоставляет концептуальную модель и инструментарий для агентно-ориентированного моделирования. В системе есть как средство разработки, так и тестирования модели. Основная идея Swarm стоит в том, чтобы разрабатывать модель в виде иерархии “роев”, которые состоят из групп объектов и запланированных действий. Java Swarm является оболочкой Java для библиотеки Swarm. Repast частично заимствует подход Swarm и реализует средства моделирования на языке Java. MASON – дискретно-событийная система многоагентного моделирования. Она позиционируется как быстрая платформонезависимая среда. NetLogo создавался как средство обучения для использования в образовательном процессе, поэтому легок в использовании. Агенты в NetLogo являются мобильными и функционируют параллельно в плоском пространстве, а их действия обуславливаются локальными взаимодействиями.

Для реализации предложенного подхода предполагалась разработка многоуровневой инструментальной среды, отличающейся от известных систем агентно-ориентированного моделирования, в первую очередь, использованием в качестве базиса средств имитационного моделирования, позволяющих адекватно имитировать сетевые протоколы и процессы. Разработанная среда моделирования имеет следующие особенности. Она

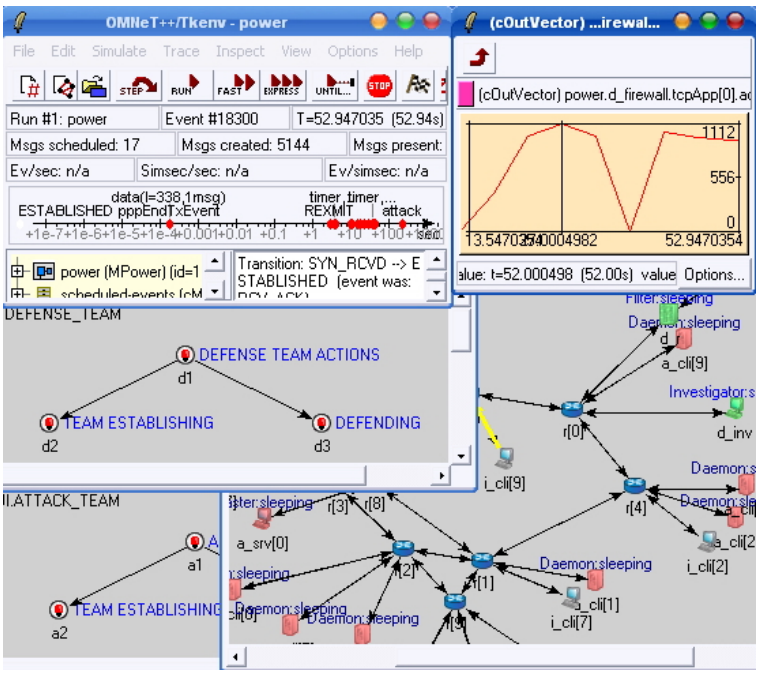

Рис. 1. Многооконный интерфейс системы моделирования

построена на базе дискретно-событийного симулятора. Вследствие этого модели агентов и их окружения представляются в виде иерархии моделей. В основе лежит система имитационного моделирования OMNeT++. Для имитации сетевых узлов и протоколов используется OMNeT++ INET Framework. Непосредственно для агентно-ориентированного моделирования разработаны библиотека Agent-based Framework и вспомогательная библиотека предметной области (DDoS Framework). Компонент агентского моделирования представляет собой библиотеку модулей, задающих интеллектуальных агентов, реализованных в виде приложений. При проектировании и реализации модулей агентов подразумевается использование элементов абстрактной архитектуры FIPA. DDoS Framework служит для имитации атак «распределенный отказ в обслуживании» и механизмов защиты от них.

Пример *многооконного пользовательского интерфейса* среды моделирования представлен на рис. 1. Окно управления процессом моделирования показано вверху слева. Справа внизу виден фрагмент моделируемой сети. На ее узлах установлены агенты различных команд. Среда позволяет наблюдать в реальном времени данные (в графическом и текстовом представлении), характеризующие функционирование того или иного компонента. Например, на рис.1 слева можно видеть окна, отображающие состояния команд агентов, а справа вверху – окно, показывающее изменение одного из параметров агента.

3. 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. На основе экспериментов проводятся измерения различных показателей эффективности механизмов защиты, и выполняется анализ условий и возможности их применения.

Сети, используемые для моделирования, состоят из различных подсетей, являющихся, например, зонами ответственности различных провайдеров. Выделяются подсеть защиты, где расположен ресурс, являющийся целью атаки, промежуточная подсеть, в которой находятся узлы, создающие типовой трафик, а также подсети атаки, где располагаются команды атаки. Сети генерируются с помощью алгоритмов, позволяющих создавать конфигурации, близкие к сети Интернет. На рис. 2 изображен фрагмент сети, использованной для проведения экспериментов. Сеть состоит из маршрутизаторов (в центре),

клиентских узлов и узлов с агентами. Выделено три команды атаки и

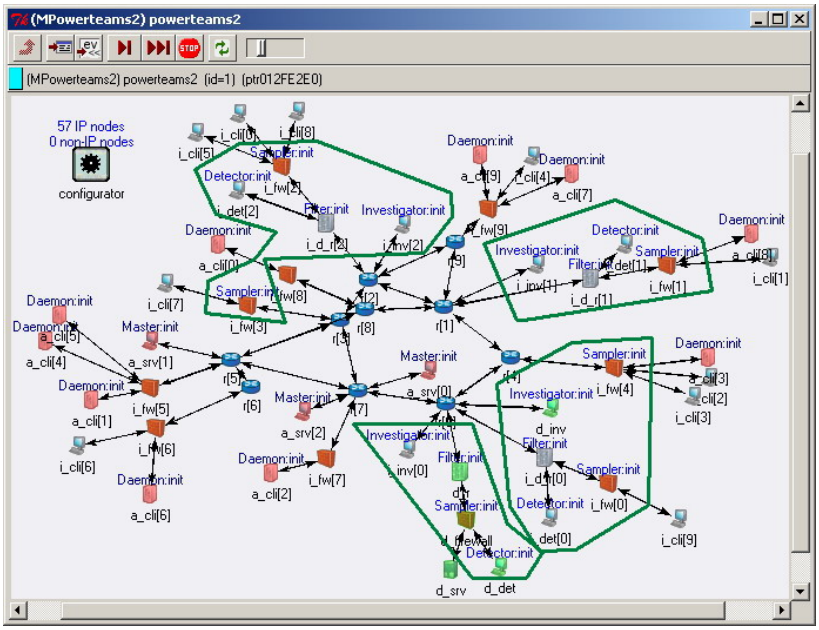

Рис. 2. Сеть, используемая для проведения моделирования

четыре команды защиты.

Для *защиты* используются методы Hop counts Filtering (HCF), Source IP address monitoring (SIPM) и Bit Per Second (BPS). Первый заключается в применении сформированных в режиме обучения таблиц подсетей и количества скачков до них. Во втором используется предположение, что во время атаки появляется большое количество новых адресов клиентов. Последний позволяет обнаружить атакующих по превышению порога нормального трафика.

Для команды атаки в процессе экспериментов варьируется интенсивность атаки в пакетах в секунду и способ подмены адреса отправителя. *Для команд защиты в процессе экспериментов варьируются* используемые методы защиты и параметр кооперации, задающий количество используемых в командах сэмплеров. Исследованы следующие *параметры эффективности механизмов защиты*: доля отброшенного легитимного трафика (false positive); доля пропущенного трафика атаки (false negative); время реакции на атаку. Параметры эффективности механизмов защиты исследовались в зависимости от следующих параметров: конфигурация команд защиты (количество

сэмплеров); конфигурация сети (количество легитимных клиентов); способ подмены адреса отправителя, используемый при атаке; интенсивность атаки.

На рис. 3 представлены *доли отброшенного легитимного трафика и пропущенных атак для трех методов защиты при различных конфигурациях команд защиты*. Эти доли являются усредненными значениями для четырех типов подмены адреса при атаке.

На рис. 3(1) показаны зависимости для метода BPS. Видно, что состав команд защиты практически не влияет на долю ложных срабатываний и пропусков атак. Это связано с тем, что сэмплеры, расположенные «вдалеке» от защищаемой сети не смогли сопоставить большой объем трафика определенным IP-адресам. Фактически, правила фильтрации были установлены лишь по информации от сэмплера в защищаемой сети, так как здесь трафик атаки достигает достаточного объема.

На рис. 3(2) изображены зависимости для метода HCF. Этот метод обнаруживает атаки только, если атакующий использует для подмены адреса из данной сети. Поэтому доли ложных срабатываний и пропусков атак представлены только для этого подвида атаки. Видно, что большое количество распределенных сэмплеров дает небольшое уменьшение пропуска атак при неизменной доли ложных срабатываний.

На рис. 3(3) изображены зависимости для метода SIPM. Видно, что при увеличении количества сэмплеров в командах защиты растет доля ложных срабатываний и при 5–6 сэмплерах устанавливается на уровне

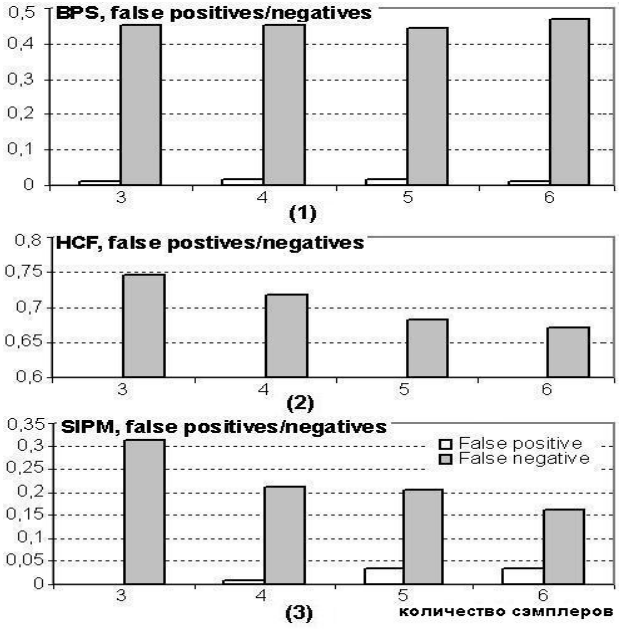

Рис. 3. Доли ложных срабатываний и пропусков атак

3%. При этом доля пропуска атак снижается почти в два раза. Следовательно, большое количество распределенных сэмплеров дает существенное уменьшение пропуска атак при небольшой доле ложных срабатываний.

Доли ложных срабатываний и пропусков атак для разных методов защиты были также исследованы при использовании только одной команды защиты, включающей детектора, фильтра, агента расследования и одного сэмплера. В результате экспериментов оказалось, что показатели механизмов защиты в такой конфигурации хуже, чем при кооперации нескольких команд с большим набором сэмплеров. Это доказывает преимущество предложенного подхода.

Заключение

В работе предложен подход к созданию команд агентов, участвующих в информационном противоборстве (на примере распределенных атак «отказ в обслуживании» и механизмов защиты от них). Подход реализован в разработанной среде моделирования, позволяющей моделировать атаки, направленные на нарушение доступности информационных ресурсов, и механизмы защиты от них.

Проведено большое количество разнообразных экспериментов, в которых исследовались параметры эффективности механизмов защиты от топологии и конфигурации сети, структуры и конфигурации команд атаки и защиты, механизмов реализации атак и защиты и параметров кооперации команд защиты. Эксперименты показали, что использования кооперации нескольких команд защиты приводит к существенному повышению эффективности защиты.

В дальнейшем планируется разработка формальных моделей поведения сложных систем в Интернет, совершенствование среды моделирования, более глубокое исследование эффективности механизмов кооперации различных команд и внутрикомандного взаимодействия агентов, реализация механизмов адаптации и самообучения агентов.

Список литературы

[Котенко и др., 2005] Котенко И.В., Уланов А.В. Агентно-ориентированное моделирование процессов защиты информации: противоборство агентов за доступность ресурсов компьютерных сетей // Труды Международных научно-технических конференций “Интеллектуальные системы (AIS'05)” и “Интеллектуальные САПР (CAD-2005)”. М.: Физматлит, 2005.

[Kotenko et al., 2005] Kotenko I., Ulanov A. Multiagent modeling and simulation of agents’ competition for network resources availability // Second International Workshop on Safety and Security in Multiagent Systems. Utrecht, The Netherlands. 2005.