УДК 681.3.053:681.32:007.5

АГЕНТНО-ОРИЕНТИРОВАННОЕ МОДЕЛИРОВАНИЕ ПОВЕДЕНИЯ СЛОЖНЫХ СИСТЕМ В СРЕДЕ ИНТЕРНЕТ*

И.В. Котенко[1], А.В. Уланов[2]

В работе предлагается подход к исследованию поведения сложных систем, функционирующих в среде Интернет, на основе агентно-ориентированного моделирования. Предполагается, что такие системы представляются в виде комплекса различных взаимодействующих команд интеллектуальных агентов, которые могут находиться между собой как в состоянии антагонистического противоборства, так и кооперации. Рассмотрена общая концептуальная модель антагонистического противоборства и кооперации команд агентов. Приведена архитектура интегрированной программной среды агентно-ориентированного моделирования. Представлена реализация среды моделирования на основе системы моделирования дискретных событий, позволившая комплексировать агентно-ориентированное моделирование с имитацией сетевых процессов на различных уровнях стека протоколов Интернет.

Введение

Ввиду ряда особенностей определенные классы систем практически не поддаются автоматизации на основе использования традиционных архитектур, методов и средств разработки программного обеспечения, и требуются новые подходы к их исследованию. Компоненты таких систем могут быть “большими”, “открытыми” системами, не полностью известными заранее, изменяющимися во времени, гетерогенными, реализоваться различными людьми, в разное время, с использованием различных средств и методов.

* 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 поддержке, осуществляемой в рамках проекта POSITIF Шестой рамочной программы Евросоюза (контракт IST-2002-002314)

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

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

Одним из наиболее известных примеров больших открытых систем является среда Интернет, представляющая собой слабосвязанную компьютерную сеть постоянно увеличивающегося размера и сложности. Проектирование и реализация программных средств для использования огромного потенциала Интернет и связанного с ней комплекса технологий – одна из наиболее важных и сложных проблем, стоящих перед исследователями области компьютерных технологий. Сеть Интернет может рассматриваться как большой, распределенный информационный ресурс с выделенными сетевыми узлами и отдельными приложениями, разрабатываемыми и реализуемыми различными организациями и пользователями. 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 агентно-ориентированных систем [Bond et al., 1988; Macal et al., 2005; Тарасов, 2002; Городецкий и др., 2005].

В качестве довода в пользу использования агентских технологий часто приводят три наиболее важные свойства агентских приложения [Bond et al., 1988]:

(1) данные, механизмы управления, знания и ресурсы распределены;

(2) система естественным образом представляется как сообщество автономных сотрудничающих компонентов;

(3) система содержит унаследованные компоненты, которые должны взаимодействовать с другими, возможно новыми программными компонентами.

Агентские технологии, и, в частности, технологии агентно-ориентированного моделирования, предоставляют возможность исследовать и создавать приложения Интернет, разработать которые с использованием традиционных подходов, было практически невозможно. Они обеспечивают и более развитые средства для концептуализации и понимания процессов, происходящих в Интернет, в частности, связанных с ведением электронного бизнеса, поиском информации, распространением вирусных эпидемий, защитой от сложных сетевых атак и др.

В работе предлагается подход и инструментальные средства для исследования поведения сложных систем, функционирующих в среде Интернет, на основе агентно-ориентированного моделирования. Подход основан на представлении сетевых систем в виде комплекса взаимодействующих команд интеллектуальных агентов, которые могут

находиться между собой как в состоянии антагонистического противоборства, так и кооперации.

В *первом разделе* описывается общий подход к агентно-ориентированному моделированию. Во *втором разделе* рассмотрен пример одной из задач исследования поведения сложных систем в среде Интернет, связанной с анализом противодействия злоумышленников и систем защиты в Интернет. В *третьем разделе* предложена архитектура среды агентно-ориентированного моделирования. В *четвертом разделе* представлены выполненная реализация среды моделирования и примеры проведенных экспериментов. В *заключении* формулируются результаты работы и направления будущих исследований.

1. Общий 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 посредством модели сети Интернет [Городецкий и др., 2005; 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.

Концептуальная модель антагонистического противоборства и кооперации команд агентов включает в себя [Городецкий и др., 2005]:

(1) онтологию приложения, содержащую множество понятий приложения и отношений между ними;

(2) протоколы командной работы агентов различных команд;

(3) модели сценарного индивидуального, группового и общекомандного поведения агентов;

(4) коммуникационный компонент, предназначенный для обмена сообщениями между агентами;

(5) модели среды функционирования – компьютерной сети, включающие топологический и функциональные компоненты.

Предлагаемый подход к организации командной работы агентов базируется на совместном использовании элементов теории общих намерений, теории разделяемых планов и комбинированных подходов [Tambe, 1997] и учитывает опыт программной реализации многоагентных систем (GRATE, OAA, CAST, RETSINA-MAS, COGNET/BATON и др. [Fan et al., 2004]).

Для формирования команд агентов и координации действий между командами и отдельными агентами в зависимости от задачи моделирования предполагается использовать комбинации следующих методов и моделей [Paruchuri et al., 2006; Kotenko et al., 2005]:

(1) традиционные BDI-модели, определяемые схемами функционирования агентов, обуславливаемыми зависимостями предметной области;

(2) методы распределенной оптимизации на основе ограничений, использующие локальные взаимодействия при поиске локального или глобального оптимума;

(3) методы распределенного принятия решений на основе частично-наблюдаемых Марковских сетей, позволяющих реализовать координацию командной работы при наличии неопределенности в действиях и наблюдениях;

(4) теоретико-игровые модели и модели аукциона, фокусирующиеся на координации среди различных команд агентов, использующих рыночные механизмы принятия решений.

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 именно эта часть знаний является тем фрагментом, который должен играть роль общего контекста (общих знаний). Структура команды агентов описывается в терминах иерархии групповых и индивидуальных ролей. Механизмы взаимодействия и координации агентов базируются на процедурах обеспечения согласованности действий, мониторинга и восстановление функциональности агентов, обеспечение селективности коммуникаций. Спецификация иерархии планов действий осуществляется для каждой из ролей. Для каждого плана описываются: начальные условия, когда план предлагается для исполнения; условия, при которых план прекращает исполняться; действия, выполняемые на уровне команды, как часть общего плана. Для групповых планов явно выражается совместная деятельность. Предполагается, что агенты могут реализовать механизмы самоадаптации и эволюционировать в процессе функционирования.

2. Пример задачи исследования поведения сложных систем в среде Интернет

Одной из актуальных задач, требующих решения для создания информационно-безопасных распределенных вычислительных систем,

является *задача формализации противодействия злоумышленников и систем защиты в сети Интернет* [Kotenko et al., 2005].

При формализации данной задачи можно выделить, по крайней мере, три различных класса команд агентов, воздействующих на компьютерную сеть, а также друг на друга: класс команд агентов-злоумышленников, класс команд агентов защиты и класс агентов-пользователей, имитирующих легитимных пользователей. Агенты различных команд могут находиться в отношении безразличия, сотрудничать для достижения одной цели и различных непротиворечивых целей, или соперничать для достижения противоположных намерений.

Цель команд агентов-злоумышленников заключается в определении уязвимостей компьютерной сети и системы защиты и реализации угроз безопасности посредством выполнения скоординированных атак. Может существовать несколько команд злоумышленников, которые в различное время могут сотрудничать между собой для достижения общей цели, находиться в отношении безразличия или соперничать за компрометацию ресурсов (вплоть до явно выраженного противоборства).

Примером соперничества является так называемая “вирусная война”, при которой каждая из команд пытается скомпрометировать хосты сети и внедрить на них свой вирус. Если одна из команд внедрила вирус, другая стремится удалить этот вирус и заменить его своим вирусом.

Цель команд агентов защиты состоит в защите сети и собственных компонентов от атак. Предполагается, что различные команды защиты сотрудничают для защиты сети Интернет.

Команды агентов-пользователей выполняют разрешенные функции по использованию ресурсов сети. Они могут сотрудничать между собой для достижения общей цели или находиться в отношении безразличия. При моделировании процессов противодействия злоумышленников и систем защиты эти команды создают стандартный (нормальный) трафик сети.

Одной из задач команд агентов защиты является защита трафика, создаваемого агентами-пользователями. Это актуально, например, при противодействии атакам, направленным на нарушение доступности. В данном случае агенты защиты, пытающиеся блокировать трафик, создаваемый агентами атаки, должны также обеспечивать беспрепятственный пропуск нормального трафика.

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.

3. Архитектура среды агентно-ориентированного моделирования

Для реализации представленного подхода предполагается разработка многоуровневой инструментальной среды, отличающейся от известных средств агентно-ориентированного моделирования (например, CORMAS, Repast, Swarm, MadKit, MASON, NetLogo и др.) [Marietto et al., 2002; Macal et al., 2005], в первую очередь, использованием в качестве базиса средств (пакетов) имитационного моделирования, позволяющих адекватно имитировать сетевые процессы. Поэтому для реализации подхода используется архитектура среды моделирования (рис.1), включающая базовую систему имитационного моделирования (Simulation Framework), модуль (пакет) моделирования сети Интернет (Internet Simulation Framework), подсистему агентно-ориентированного моделирования (Agent-based Framework) и модуль (библиотеку) имитации процессов предметной области (Subject Domain Library).

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

Рис.1. Архитектура среды моделирования

Компонент Internet Simulation Framework – комплект модулей, позволяющих реалистично моделировать узлы и протоколы сети

Интернет. Наивысший уровень абстракции в моделировании IP – это сеть, состоящая из IP-узлов. Узел может быть маршрутизатором или хостом. IP-узел отвечает компьютерному представлению стека протоколов Интернет. Предполагается, что 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 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 архитектуры FIPA. 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.

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

4. Реализация среды моделирования и эксперименты

На основе OMNeT++ INET Framework разработана среда для многоагентного моделирования сложных систем в сети Интернет на примере *противодействия злоумышленников и систем защиты в сети Интернет по реализации* распределенных компьютерных атак и механизмов защиты от них. Система разработана на основе OMNET++ INET Framework на языке C++. Архитектура реализованной среды соответствует архитектуре, представленной на рис.1. 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). Пример многооконного пользовательского интерфейса интегрированной среды моделирования представлен на рис.2. В данном случае отображено окно компьютерной сети (справа вверху), окно управления процессом моделирования (внизу справа), окна, характеризующие состояние команд агентов (вверху слева),

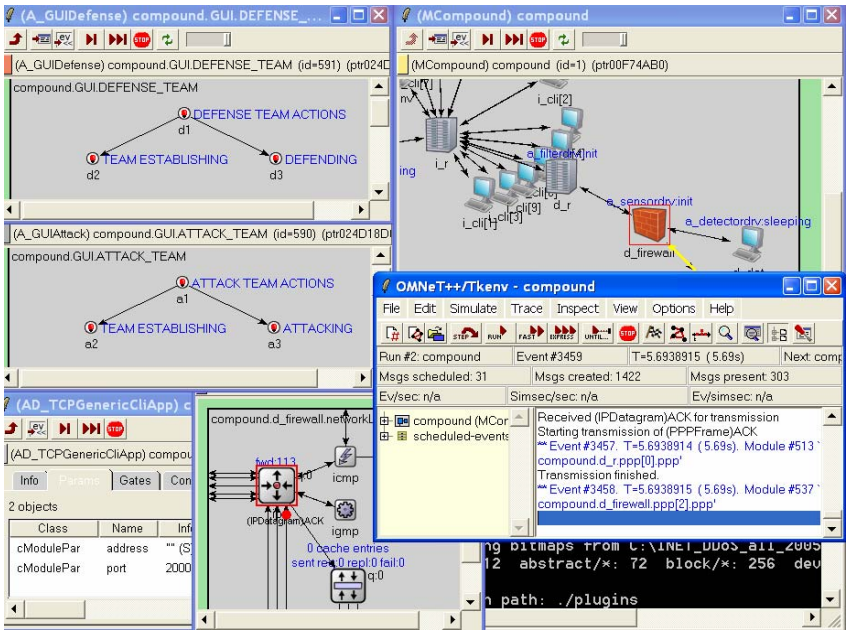

Рис.2. Пример пользовательского интерфейса среды моделирования

окно параметров агента (внизу слева), окно функционирования отдельного хоста (внизу в центре).

В среде моделирования проведен ряд экспериментов с использованием конфигураций компьютерных сетей, близких по топологии к фрагментам Интернет. Сеть состоит из трех подсетей. В первой подсети устанавливается команда атаки, включающая агентов-демонов и агента-мастера. Демоны являются непосредственными исполнителями атаки. Мастер координирует их действия. Во второй – клиенты, создающие типовой сетевой трафик к защищаемому узлу. В третьей подсети определен узел-цель атаки, и установлена команда защиты: сэмплер, детектор, фильтр и агент расследования. Агенты-сэмплеры осуществляют мониторинг сетевых процессов с целью выявления аномалий и начала атаки. Агенты обнаружения служат для выявления атак. Агенты фильтрации осуществляют фильтрацию трафика от вредоносных пакетов. Агенты расследования выполняют трассировку атак, выявление агентов атаки и выполненной ими злонамеренной деятельности. Моделирование продолжается до заданного момента времени, отражая различные шаги противоборствующих команд агентов.

Заключение

В работе предложен подход к моделированию поведения сложных систем в Интернет. Он может быть использован в задачах информационной борьбы в Интернет, конкуренции в сфере электронного бизнеса и др. Рассмотрена архитектура среды моделирования, использующая предложенный подход. На основе OMNeT++ INET Framework разработана среда для агентно-ориентированного моделирования на примере распределенных атак и механизмов защиты от них. Она позволяет моделировать большой спектр атак, направленных на нарушение доступности информационных ресурсов, и механизмов защиты от них. Дальнейшее развитие работы связано с разработкой формальных моделей поведения сложных систем в Интернет, совершенствованием среды моделирования (в том числе на основе реализации других задач поведения сложных систем в Интернет), исследованием эффективности механизмов внутрикомандного взаимодействия агентов, реализацией механизмов адаптации и самообучения агентов.

Список литературы

[Городецкий и др., 2005] В.Городецкий, И.Котенко. Концептуальные основы стохастического моделирования в среде Интернет // Труды института системного анализа РАН, том 9: Фундаментальные основы информационных технологий и систем. – М.: УРСС, 2005.

[Тарасов, 2002] Тарасов В.Б. От многоагентных систем к интеллектуальным организациям: философия, психология, информатика. – М.: УРСС, 2002.

[Bond et al., 1988] A.H.Bond, L.Gasser (Eds.). Readings in Distributed Artificial Intelligence. Morgan Kaufmann. 1988.

[Fan et al., 2004] Fan X., Yen J. Modeling and Simulating Human Teamwork Behaviors Using Intelligent Agents // Journal of Physics of Life Reviews, Vol. 1, No. 3. 2004.

[Jennings, 2001] Jennings N.R. Building complex, distributed systems: the case for an agent-based approach // Communications of the ACM, 44 (4). 2001.

[Kotenko et al., 2005] Kotenko I.V., Ulanov A.V. Agent-based simulation of DDOS attacks and defense mechanisms // Journal of Computing, Vol. 4, Issue 2. 2005.

[Macal et al., 2005] Macal C.M., North M.J. Tutorial on Agent-based Modeling and Simulation // Proceedings of the 2005 Winter Simulation Conference. WSC'05. 2005.

[Marietto et al., 2002] Marietto M., David N., Sichman J.S., Coelho H. Requirements Analysis of Agent-Based Simulaton Platforms: State of the Art and New Prospects // Multi-Agent-Based Simulation II, Vol. 2581 of LNAI series, Springer-Verlag. 2002.

[Paruchuri et al., 2006] Paruchuri P., Bowring E., Nair R., Pearce J.P., Schurr N., Tambe M., Varakantham P. Mutiagent Teamwork: Hybrid Approaches // Computer society of India Communications. 2006.

[Tambe, 1997] Tambe M. Towards flexible teamwork // Journal of AI Research. Vol.7. 1997.