# МОДЕЛИРОВАНИЕ АДАПТИВНЫХ КООПЕРАТИВНЫХ СТРАТЕГИЙ ЗАЩИТЫ ОТ КОМПЬЮТЕРНЫХ АТАК В СЕТИ ИНТЕРНЕТ*

**А. В. Уланов, И. В. Котенко (Санкт-Петербург)**

В соответствии с современными представлениями, перспективная система защиты компьютерных сетей от сетевых атак должна интегрировать различные распределенные механизмы защиты, быть адаптивной и динамически эволюционировать при изменении условий работы. Поэтому очень важно разрабатывать гибкие, кооперативные, адаптивные, распределенные механизмы защиты от сетевых атак, а также определять оптимальные стратегии защиты с помощью исследовательского моделирования.

Одним из наиболее серьезных типов атак является атака «распределенный отказ в обслуживании» (Distributed Denial of Service, DDoS). Она нацелена на перегрузку хоста или сетевого ресурса посредством наполнения системы – цели атаки большим количеством сетевых пакетов. Эти атаки реализуются большим количеством программных агентов («ботов» или «демонов»), размещенных на хостах, которые злоумышленник скомпрометировал ранее. Эффективная защита от атак DDoS, которая включает предупреждение, определение факта, обнаружение источника и противодействие атаке, является очень сложной задачей. Основная задача защиты состоит в точном определении атак DDoS, быстром реагировании на них, распознавании легитимного трафика, который смешан с трафиком атаки, и доставке его до цели атаки [1]. Адекватная защита может быть достигнута только с помощью кооперации различных распределенных компонентов.

*Авторами предлагается многоагентный подход и программная среда моделирования для имитации противодействия систем защиты злоумышленникам. Среда и подход предназначены, в первую очередь, для исследования кооперативных адаптивных систем защиты от атак DDoS.*

## Релевантные работы и особенности предлагаемого подхода

Для реализации представленного подхода предполагалась разработка среды многоагентного моделирования, отличающейся от известных *средств агентно-ориентированного моделирования* (например, CORMAS, Repast, Swarm, MadKit, MASON, NetLogo и др.) [2] в первую очередь использованием в качестве базиса средств имитационного моделирования, позволяющих адекватно имитировать сетевые протоколы и процессы информационной безопасности. С другой стороны, существует ряд средств, которые могут быть использованы для *имитации компьютерных сетей*: NS2, OMNeT++ INET Framework, SSF Net, J-Sim и т. д. Для выбора средств моделирования авторами выполнен детальный анализ сред моделирования [3].

*Традиционная защита от атак DDoS* включает механизмы обнаружения и реагирования. Для обнаружения аномальных сетевых характеристик могут быть применены многие методы (например, статистические, кумулятивных сумм, сравнение паттернов и т.д.). Примерами таких *методов обнаружения* являются Hop counts Filtering (HCF), Source IP address monitoring (SIPM), Bit per Second (BPS) и т. п [4]. Как правило, *механизмы реагирования* включают фильтрацию, контроль нагрузок и отслеживание. Так как обнаружение атак DDoS наиболее точно, когда оно производится рядом с целью атаки, а отделение легитимного трафика наиболее успешно рядом с источниками

* 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 проектов Евросоюза POSITIF (контракт IST-2002-002314) и RE-TRUST (контракт № 021186-2).

атаки, адекватная защита по сдерживанию трафика атаки может быть достигнута только на основе кооперации различных компонентов. Существует множество архитектур для кооперативной распределенной защиты [4].

*Задача адаптации* рассмотрена в большом количестве статей [5]. Ряд из них посвящен реализации адаптивного подхода к защите от атак DDoS. В отчете [6] рассматривается способность динамического изменения поведения для поддержки работы сетевых сервисов во время атаки DDoS. Система Saber [7] использует для согласованной защиты различные механизмы: обнаружение вторжений, автоматическую установку заплат (патчей), миграцию процессов и фильтрацию атак. В [8] рассматривается подход и система для гранулярно-адаптивного обнаружения атак. В [9] сформулирован принцип адаптивной защиты на основе минимизации «стоимости» защиты, а также предложены адаптивные модели защиты.

*Подход, предлагаемый в настоящей работе*, основан на представлении сетевых систем в виде комплекса команд взаимодействующих агентов, которые могут быть в состоянии антагонистического противостояния, безразличия или кооперации. Агрегированное поведение системы выражается в локальных взаимодействиях агентов. Поведение антагонистических команд основано на использовании некоторого *критерия адаптации*. В соответствии с этим критерием антагонистические команды (системы атаки и защиты) настраивают свою конфигурацию и поведение в соответствии с условиями сети и поведением соперничающей команды, например, в зависимости от серьезности (мощности) атаки и защиты.

**Модели команд агентов и среда моделирования**

В работе используется следующая структура и функциональность команд атаки и защиты [3]. *Агенты атаки* подразделяются, по крайней мере, на два класса: «демоны», непосредственно реализующие атаку, и «мастер», координирующий остальные компоненты системы. Режим атаки определяется, например, интенсивностью посылки пакетов (пакетов в секунду) и способом подмены адреса отправителя в пакете («IP spoofing»). В соответствии с общим подходом к *защите от атак DDoS* выделены следующие классы агентов защиты [3]: обработки информации («сэмплеры»), обнаружения атаки («детекторы»); фильтрации и балансировки нагрузки («фильтры»); расследования и деактивации агентов атак («агенты расследования»).

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. 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.

Архитектура среды моделирования включает четыре основных компонента. *Компонент Simulation Framework* представляет собой систему моделирования на основе дискретных событий. *Компонент Internet Simulation Framework* – комплект модулей, позволяющих моделировать узлы и протоколы сети Интернет. Многоагентное моделирование реализуется посредством *компонента Agent-based Framework*, который использует модуль имитации процессов предметной области. *Компонент Subject Domain Library* – библиотека, служащая для имитации процессов предметной области.

Представленная архитектура была реализована с использованием OMNeT++ INET Framework [10] и программных моделей, разработанных на C++. Модели агентов, реализованные в Agent-based Framework, представлены типовым агентом, агентами

атаки и агентами защиты. Используются следующие *спецификации для задания исследуемых моделей сети, механизмов защиты и атаки*: топология сети; конфигурация команд атаки; параметры реализации атаки; параметры команды защиты; схема адаптации (изменения механизмов защиты) в зависимости от успешности атаки и т.п.; параметры механизмов защиты; параметры команды пользователей; параметры кооперации агентов защиты; параметры моделирования.

**Механизмы адаптации и обучения**

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 политики безопасности, формирования новых экземпляров механизмов и профилей защиты. Общий принцип адаптации команды защиты заключается в следующем [9]: при изменении режима атаки подсистема адаптации выбирает конфигурацию системы защиты, которая минимизирует функцию эффективности:

$$\min_{S(t)} \sum_{i=1}^{n} C_i(S(t), K_D(t)),$$

где $S(t)$ – показатель мощности атаки на время $t$; $K_D(t) = \{M_\text{i}, TK_\text{j}\}$ – конфигурация системы защиты на время $t$; $TK_\text{j}$ – схема кооперации механизмов защиты; $C_i(\text{S}(t),K_D(t))$ – $i$-й компонент стоимости защиты от атаки ($i$=1,…,$n$).

В проводимых экспериментах принимается следующий критерий адаптации:

$$\min_{S(t)}\{C_{FP}(S(t), K_D(t)) + C_{FN}(S(t), K_D(t)) + C_T(S(t), K_D(t))\},$$

где $C_{FP}(S(t), K_D(t))$ – процент ложных срабатываний системы защиты; $C_{FN}(S(t), K_D(t))$ – процент пропуска атак системы защиты; $C_T(S(t), K_D(t))$ – продолжительность атаки.

*Команда атаки* старается максимизировать затраты команды защиты. В экспериментах принимается следующий критерий адаптации команды атаки:

$$\min_{E(t)}\{C_P(E(t), K_A(t)) + C_D(S(t), K_A(t))\},$$

где $E(t)$ – показатель действенности защиты на время $t$; $K_A(t)= \{I_\text{i}, R_\text{j}\}$ – параметры атаки на время $t$ (здесь $I_\text{i}$ – интенсивность атаки, $R_\text{j}$ – метод подмены адреса отправителя); $C_\text{j}(E(t),K_A(t))$ – $j$-й компонент стоимости атаки ($j$=1,…,$m$); $C_P(E(t), K_A(t))$ – количество посланных пакетов; $C_D(E(t), K_A(t))$ – количество обезвреженных демонов.

**Эксперименты**

В проведенных имитационных экспериментах *команда атаки* начинает атаку в заданный момент времени с заданными интенсивностью и методом подмены адреса отправителя. Периодически мастер опрашивает демонов. Если мастер обнаруживает, что какой-то из них неработоспособен, он перераспределяет нагрузку в соответствии с заданной интенсивностью атаки, изменяет метод подмены адреса отправителя и рассылает эти параметры оставшимся демонам.

*Команда защиты* изначально функционирует, используя наименее ресурсоемкий способ защиты. Как только обнаруживается атака, делается попытка заблокировать пакеты от атакующих, проследить их и обезвредить. Если после совершения этих действий регистрируется атака, то детектор изменяет метод защиты на более сложный (в

соответствии с функцией адаптации) и рассылает команду изменения метода остальным агентам.

Схема адаптации тестируется в различных режимах кооперации, описанных ниже. В режиме кооперации на уровне сэмплеров и при полной кооперации предполагается кооперативное обучение команд. Исследуются следующие *схемы*: 1) *без кооперации*; 2) *кооперация на уровне фильтров*: команда, на сеть которой направлена атака, может применять правила фильтрации на фильтрах других команд; 3) *кооперация на уровне сэмплеров*: команда, на сеть которой направлена атака, может получать информацию о трафике от сэмплеров других команд; 4) *слабая кооперация*: команды могут получать информацию о трафике от сэмплеров некоторых других команд и применять правила фильтрации на фильтрах также некоторых других команд; 5) *полная кооперация*: команда, на сеть которой направлена атака, может получать информацию о трафике от всех сэмплеров других команд и применять правила фильтрации на всех фильтрах других команд.

Исследование проводилось на основе анализа следующих *основных параметров*: величина входного трафика до и после фильтра команды, чья сеть под атакой; процент нормального трафика и трафика атаки от всего трафика перед входом в атакуемую сеть; процент ложных срабатываний и пропусков атак команды, чья сеть под атакой. Эксперименты показали, что наилучшие результаты в адаптивной блокировке трафика атаки можно достичь при кооперации команд защиты, при этом лучшая адаптивная схема – с кооперацией на уровне сэмплеров и с полной кооперацией.

**Заключение**

Предлагается многоагентный подход к моделированию перспективных адаптивных и кооперативных механизмов информационной безопасности в сети Интернет. Среда для многоагентного моделирования разработана на базе OMNeT++ INET Framework. Пример реализованного сценария моделирования заключается в реализации кооперативных адаптивных стратегий DDoS атак и защиты от них. Проведенные эксперименты показали возможность использования предложенного подхода для моделирования механизмов защиты и для анализа проектируемых сетей. Они продемонстрировали также, что использование кооперации нескольких команд защиты и комбинированного адаптивного применения различных методов защиты ведет к существенному повышению ее эффективности.

Дальнейшее направление исследований связано с более глубоким анализом эффективности кооперативных механизмов защиты, реализацией механизмов улучшенной адаптации и самообучения агентов, подверженных действиям атакующих, расширением библиотек атаки и защиты, анализом новых механизмов защиты.

**Литература**

1. **Mirkovic J., Dietrich S., Dittrich D., Reiher P.** Internet Denial of Service: Attack and Defense Mechanisms. Prentice Hall PTR, 2004.
2. **Macal C. M., North M. J.** Tutorial on Agent-based Modeling and Simulation// Proceedings of the 2005 Winter Simulation Conference. Orlando, FL, USA, 2005.
3. **Kotenko I., Ulanov A.** Simulation of Internet DDoS Attacks and Defense // Proceedings of 9th Information Security Conference (ISC 2006). Samos, Greece, 2006. Lecture Notes in Computer Science. Vol. 4176.
4. **Уланов А. В., Котенко И. В.** Защита от DDoS-атак: механизмы предупреждения, обнаружения, отслеживания источника и противодействия//Защита информации. Инсайд, 2007. № 1–3.

5. **Kotenko I., Ulanov A.** Multi-agent Framework for Simulation of Adaptive Cooperative Defense Against Internet Attacks//Proc. of the Second International Workshop, AIS-ADM 2007. St.Petersburg, Russia, June 3–5, 2007.
6. **Piszcz A., Orlans N., Eyler-Walker Z., Moore D.** Engineering Issues for an Adaptive Defense Network. MITRE Technical Report. 2001.
7. **Keromytis A. D., Parekh J., Gross P. N., Kaiser G., Misra V., Nieh J., Rubensteiny D., Stolfo S. A.** Holistic Approach to Service Survivability//Proceedings of ACM Workshop on Survivable and Self-Regenerative Systems. Fairfax, VA, 2003.
8. **Gamer T., Scholler M., Bless R.** A Granularity-adaptive System for in-Network Attack Detection//Proceedings of the IEEE/IST Workshop on Monitoring, Attack Detection and Mitigation. Tuebingen, Germany, 2006.
9. **Zou C. C., Duffield N., Towsley D., Gong W.** Adaptive Defense against Various Network Attacks // IEEE Journal on Selected Areas in Communications: High-Speed Network Security (J-SAC). 2006. Vol. 24, No. 10.
10. OMNeT++ homepage. http://www.omnetpp.org