Котенко И.В., Уланов А.В.

ИССЛЕДОВАНИЕ МЕХАНИЗМОВ ЗАЩИТЫ ОТ АТАК DDOS: ИМИТАЦИЯ ПРОТИВОБОРСТВА ИНТЕЛЛЕКТУАЛЬНЫХ АГЕНТОВ В СЕТИ ИНТЕРНЕТ

Санкт-Петербург, СПИИРАН

Ввиду критичности класса атак «распределенный отказ в обслуживании» (DDoS), сложности проведения исследований по анализу данных атак и механизмов защиты от них на реальных сетях, актуальной и важной задачей является имитационное моделирование таких механизмов защиты.

В работе предлагается подход к исследованию атак DDOS и механизмов защиты от них. В его основу положено представление сторон атаки и защиты в виде команд интеллектуальных агентов, которые могут противоборствовать, кооперироваться и адаптироваться к действиям друг друга [1, 2].

Разработанная модель команды атаки включает два класса агентов:
- «демон», непосредственно реализующий атаку, и
- «мастер», выполняющий действия по координации остальных компонентов системы.

Предложены различные классы агентов защиты:
- первичной обработки информации («сэмплеры»);
- обнаружения атаки («детекторы»);
- фильтрации («фильтры»);
- ограничения трафика («ограничители»);
- агенты расследования.

Разработаны различные модели взаимодействия команд [3, 4]:
- антагонистическое противоборство,
- кооперативная защита,
- адаптивная схема.

На основе данного подхода разработана программная среда (система) моделирования механизмов защиты от атак DDOS.

Архитектура системы моделирования включает (рис.1):
- базовую систему имитационного моделирования,
- модуль (пакет) моделирования сети Интернет,
- подсистему агентно-ориентированного моделирования и
- модуль (библиотеку) имитации процессов предметной области.

С использованием OMNeT++ INET Framework и программных моделей, разработанных на C++, представленная архитектура была реализована для многоагентного моделирования механизмов защиты от атак DDoS.

Пользовательский интерфейс среды моделирования показан на рис.2. На рис. 2 отображено окно компьютерной сети, окно управления процессом моделирования, окна, характеризующие состояние и параметры команд агентов, окно параметров сети, окна функционирования отдельного хоста и агента.

Рис. 1. Архитектура системы моделирования

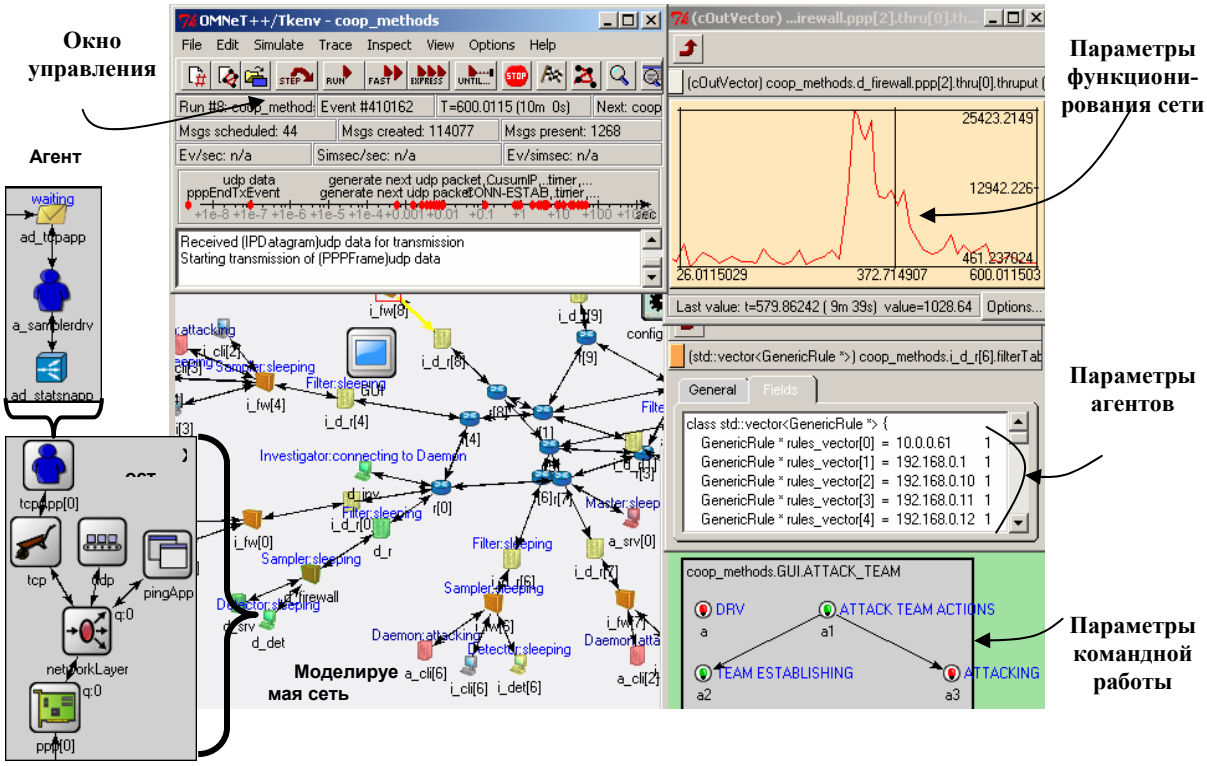

Рис. 2. Пользовательский интерфейс среды моделирования

Предложена методика анализа механизмов защиты и на основе нее проведено множество экспериментов по исследованию их эффективности.

Основными этапами разработанной методики проведения многоагентного моделирования механизмов защиты от атак DDoS: подготовительный этап, этап задания параметров, этап реализации процессов моделирования и этап анализа выходных параметров.

Основным содержанием доклада является результаты экспериментов по анализу атак DDoS и механизмов защиты от них.

В работе проведено исследование как локальных механизмов защиты - HCF (Hop Count Filtering, фильтрация по количеству «хопов»), Source IP Address Monitoring (мониторинг IP-адресов отправителей), BPS (Bit Per Second, бит в секунду), так и кооперативных механизмов защиты - DefCOM, COSSACK и различных механизмов, предложенных на основе кооперации агентов различной специализации.

Также исследовано применение различных критериев адаптации команд защиты и атаки к действиям друг друга. Исследования показали высокую практическую значимость предложенного подхода и разработанных программных средств для анализа защищенности реальных сетей от атак DDoS и исследования новых механизмов защиты.

Полученные результаты могут быть использованы для анализа систем защиты существующих сетей, а также для выработки рекомендаций по созданию перспективных систем защиты.

В дальнейшем планируется обобщение моделей для других задач информационного противоборство в Интернет, реализация новых типов атак и соответствующих механизмов защиты, увеличение точности и достоверности моделирования за счет использования гибридного подхода, а также проведение большого количества экспериментов.

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).

Литература

1. Городецкий В., Котенко И. Концептуальные основы стохастического моделирования в среде Интернет // Труды института системного анализа РАН. Т. 9. М.: УРСС, 2005.

2. Kotenko I., Ulanov A. Simulation of Internet DDoS Attacks and Defense // 9th Information Security Conference. ISC 2006. Lecture Notes in Computer Science, Vol. 4176, 2006.

3. Kotenko I., Ulanov A. Multi-agent Framework and Environment for Simulation of Adaptive Cooperative Defense against Internet Attacks // Proceedings of International Workshop on Autonomous Intelligent Systems: Agents and Data Mining (AIS-ADM-07). Lecture Notes in Artificial Intelligence, Vol.4476, 2007.

4. Котенко И.В., Уланов А.В. Многоагентное моделирование защиты информационных ресурсов в сети Интернет // Известия РАН. Теория и системы управления, 2007, № 5. С.74–88.