Многоагентная среда для проведения экспериментов по защите компьютерных сетей

Уланов А. В., Котенко И. В.
ulanov@iias.spb.su, ivkote@iias.sbp.su
Санкт-Петербург, Институт информатики и автоматизации РАН

В работе предлагается подход и реализованная среда многоагентного моделирования для анализа существующих и перспективных методов защиты от атак «распределенный отказ в обслуживании». Подход базируется на представлении систем, реализующих компьютерные атаки и защиту от них, в виде команд интеллектуальных агентов. В работе реализован ряд методов кооперативной защиты и проведено исследование их эффективности.

Защита от атак DDoS

Один из наиболее опасных классов атак в Интернете — это атака «распределенный отказ в обслуживании» (Distributed Denial of Service, DDoS). Предполагается, что перспективная система защиты от DDoS должна работать на основе кооперации различных систем, сетей и глобальных механизмов защиты, расположенных как в отдельных подсетях, так и в Интернете.

К распределенным кооперативным механизмам DDoS защиты [1] относятся: перенос ресурсов (Server Roaming), изменение количества ресурсов, дифференциация ресурсов (Market-based Service Quality Differentiation (MbSQD), Transport-aware IP router architecture), аутентификация (Secure Overlay Services (SOS)), а также механизмы, реализующие отслеживание (Gateway-based mechanism) с помощью разметки пакетов, хранения сигнатур или генерации служебных пакетов.

Цель данной работы заключается в разработке среды моделирования для исследования атак и механизмов защиты (на примере DDoS) и формулировании обоснованных рекомендаций по выбору эффективных механизмов защиты. В докладе рассматриваются предложенные подход, разработанная среда моделирования и проведенные эксперименты по исследованию интеллектуальных кооперативных механизмов защиты.

Подход и модели защиты

Предлагаемый подход к моделированию заключается в следующем. Исследуемые процессы рассматриваются как взаимодействие команд программных агентов в динамической среде, заданной посредством модели сети Интернет [2]. Поведение системы проявляется в локальных взаимодействиях отдельных агентов.

Существует, по крайней мере, три класса команд агентов: злоумышленники, команда защиты и агенты-пользователи. Агенты различных ко-

манд могут быть в состоянии безразличия, кооперироваться или соперничать.

Выделено два класса агентов команды атаки: «демон» — исполнитель атаки, «мастер» — координатор команды. В соответствии с общим подходом к защите от атак DDoS [1, 2], выделены следующие классы команды защиты: «сэмплер» — обработка данных трафика, «детектор» — обнаружение атаки, «фильтр» — фильтрация трафика, «ограничитель» — ограничение трафика, агент «расследования». Команда защиты совместно реализует определенный механизм защиты. Различные команды защиты могут взаимодействовать по разным схемам.

В работе продемонстрировано функционирование следующих механизмов защиты, осуществляющих классификацию вредоносного трафика на основе построенной модели нормального трафика [1]: Count Filtering (HCF), Source IP address monitoring (SIPM), Bit per Second analysis (BPS). В HCF используется предположение, что пакеты из одной подсети проходят одинаковое количество скачков (хопов) от отправителя до получателя. SIPM построен на том, что в начале атаки появляется много пакетов от новых для системы отправителей. BPS определяет атаку по превышению заданного порога трафика.

Для построения модели нормального сетевого трафика используется следующий способ. Легитимные клиенты обращаются к защищаемому серверу, а он обрабатывает их запросы, таким образом создавая выборку нормального трафика. Аналогичным образом создается выборка вредоносного трафика, при этом задействуются атакующие агенты команды атаки. При обучении настраиваются внутренние параметры методов защиты, такие как интервал получения данных о трафике и сдвиг этого интервала.

Основное внимание в кооперативных механизмах защиты уделяется методам распределенной фильтрации и ограничения трафика. Проведено моделирование следующих кооперативных механизмов: DefCOM, COSSACK и пяти предложенных классов. Предложены такие схемы кооперации: без кооперации, на уровне фильтров, на уровне сэмплеров, слабая кооперация и полная кооперация.

Среда моделирования и эксперименты

Предложенный подход предполагает разработку среды моделирования, архитектура которой включает следующие компоненты [2]: базовая среда моделирования, пакет имитации сети Интернет, среда многоагентного моделирования, библиотека предметной области. Первый компонент является базовым для остальных.

Данная архитектура была реализована для многоагентного моделирования распределенных механизмов защиты с использованием базовой

системы моделирования дискретных событий OMNeT++, симулятора сетей INET Framework и программных моделей, разработанных на C++.

Модель противоборства в среде моделирования задается следующими параметрами: топологией и конфигурацией сети, конфигурацией команд атаки, параметрами атак DDoS, конфигурацией команд защиты, параметрами защиты от DDoS, параметрами кооперации команд. В качестве исследуемых выходных параметров механизмов защиты рассматриваются: количество ложных срабатываний; количество пропусков атак; процент трафика атаки и нормального трафика в исследуемой сети; время реакции и др.

Исследуемые механизмы защиты основаны на реализации режимов обучения и собственно защиты с обновлением данных. В режиме обучения производится сбор данных по заведомо легитимному трафику. В режиме защиты, на основе сравнения текущих данных с модельными, выполняется обработка сетевого трафика. Несоответствие считается аномалией или атакой, и принимаются контрмеры. Если аномалий не обнаружено или они малы, то данные заносятся в модель, то есть происходит ее обновление.

Заключение

С использованием разработанной среды моделирования проведено множество экспериментов по исследованию различных типов атак, нахождению оптимальных параметров механизмов защиты, сравнению различных механизмов защиты, режимов кооперации и механизмов адаптации команд агентов. В дальнейшем планируется совершенствование среды моделирования, расширение библиотеки предметной области и системы многоагентного моделирования. Работа выполняется при финансовой поддержке РФФИ (проект № 07-01-00547), программы фундаментальных исследований ОИТВС РАН (контракт № 3.2/03) и Фонда содействия отечественной науке.

Литература

[1] *Уланов А. В., Котенко И. В.* Защита от DDoS-атак: механизмы предупреждения, обнаружения, отслеживания источника и противодействия // Защита информации. Инсайд. — 2007. — № 1 — 3.

[2] *Котенко И. В., Уланов А. В.* Команды агентов в кибер-пространстве: моделирование процессов защиты информации в глобальном Интернете // Сборник Института системного анализа РАН. — М.: URSS, 2006.