ТЕОРЕТИКО-МНОЖЕСТВЕННОЕ ПРЕДСТАВЛЕНИЕ ИМИТАЦИОННЫХ МОДЕЛЕЙ ИНФРАСТРУКТУРНЫХ АТАК И МЕХАНИЗМОВ ЗАЩИТЫ ОТ НИХ*

А. В. Шоров, И. В. Котенко (Санкт-Петербург)

В настоящее время наблюдается тенденция к увеличению количества и мощности компьютерных атак на инфраструктуру вычислительных сетей. Постоянный рост распределенных атак типа «отказ в обслуживании» и вирусных эпидемий, провоцируемых сетевыми червями, свидетельствует о необходимости исследования новых методов защиты с принципиально новой архитектурой. Такое исследование невозможно проводить на реальных компьютерных сетях в силу возможных последствий имитации атак для информационно-телекоммуникационных систем.

Таким образом, одной из важнейших задач в области защиты информации является исследовательское моделирование инфраструктурных атак и механизмов защиты от них с целью разработки и тестирования эффективных методов противодействия им. Имитационное моделирование предоставляет гибкий механизм исследования таких сложных динамических систем как системы защиты информации компьютерных сетей, позволяя оперировать с различными наборами параметров и сценариев атак и защиты.

Одним из подходов к спецификации исследуемых процессов и систем является теоретико-множественное представление. В настоящей работе предлагается теоретико-множественный подход для описания моделей инфраструктурных атак на компьютерные сети и механизмов защиты от них и проводится формализация инфраструктурных атак, механизмы защиты от них, а также среды их взаимодействия (компьютерной сети). Также рассматриваются среда имитационного моделирования, в которой реализуются представленные формальные модели, и эксперименты, проводимые с использованием данной среды. В виду ограниченности объема данной работы все модели специфицируются только на верхнем уровне представления.

Модель компьютерной сети. Представим верхний уровень модели анализируемой компьютерной сети в виде кортежа $N =< T, TP, TR >$, где T – тип топологии; TP – топология сети; TR – трафик в сети.

Тип топологии сети может быть задан как $T \subseteq \langle Ln, Bs, St, Rn, Tr, Mh, Hbr \rangle$, специфицируя следующие типы топологий: Ln – линия, Bs – шина, St – звезда, Rn – кольцо, Tr – дерево, Mh – решетка, Hbr – гибридная.

Топология сети $TP = \langle H, L \rangle$ включает в себя: H – узлы (хосты) вычислительной сети, L – связи между узлами вычислительной сети.

Трафик TR определим в виде $TR = \cup p_i^P$, где p_i – пакеты трафика, P – протокол, который используется для передачи пакета p. $p_i = \{Par_i\}$, где Par – параметры пакета в соответствии с используемым протоколом.

Например, для пакетов, инкапсулированных в соответствии с протоколом IP, $p_i^{IP} = \{srcAddr, dstAddr, AP\}$, а для пакетов на основе протокола TCP – $p_i^{TCP} = \{srcPort, destPort, AP\}$, где *srcAddr, dstAddr, srcPort, destPort* – основные параметры протоколов IP/TCP (адреса и порты источника и назначения), *AP* – дополнитель-

* Работа выполняется при финансовой поддержке РФФИ (проект 10-01-00826-а), программы фундаментальных исследований ОНИТ РАН (проект 3.2), государственного контракта 11.519.11.4008 и при частичной финансовой поддержке, осуществляемой в рамках проектов Евросоюза SecFutur и MASSIF.

ные атрибуты пакета, включая полезную нагрузку. Множество пакетов p_i^P генерируется множеством приложений PO.

Модели инфраструктурных атак. Множество моделей инфраструктурных атак на верхнем уровне представляются в следующем виде: $A = \langle TA, CA \rangle$, где TA – тип инфраструктурной атаки, CA – параметры реализации атаки.

Тип инфраструктурной атаки может задаваться в следующем виде: $TA = \langle Wrm_{n,m}, DDoS_{n,m}, AoR_{n,m}, AoDNS_{n,m} \rangle$, где $Wrm_{n,m}$ – распространение сетевого червя, $DDoS_{n,m}$ – распределенная атака типа «отказ в обслуживании», $AoR_{n,m}$ – атаки на маршрутизаторы, $AoDNS_{n,m}$ – атаки на DNS-сервера; переменная *n* служит для идентификации типа атаки на верхнем уровне представления модели (например, название типа атаки), *m* определяет параметры заданного механизма атаки (например, источник атаки).

Опишем модели сетевого червя и распределенной атаки типа «отказ в обслуживании», как наиболее часто выполняемых инфраструктурных атак.

Определим сетевого червя с помощью теоретико-множественных моделей:

$Wrm_{n,m} = \langle I,\ M_{ct},\ f, Sprt,\ Dprt, M_{st}, P_{sc}, PS,\ M_{spoof} \rangle$, где I – идентификатор червя; M_{ct} – тип соединения, соединения могут быть на основе протокола TCP или на основе протокола UDP; f –частота генерации пакетов, число пакетов (соединений), генерируемых в секунду; $Sprt$ – сетевой порт, с которого отсылаются пакеты; $Dprt$ – сетевой порт, на который отсылаются пакеты; M_{st} – методика сканирования; P_{sc} – вероятность установления успешного TCP-соединения. Данный параметр имеет значение в случае распространения сетевого червя по протоколу TCP; в случае работы по UDP параметр помечается как недоступный; PS – размер пакета, передаваемого по сети; M_{spoof} – методики подмены сетевого адреса и порта.

Далее опишем модель DDoS-атаки:

$DDoS_{n,m} = \langle I, TDD, NP, f, Sprt, Dad, Dprt, PS, M_{spoof} \rangle$, где I – идентификатор атаки; *TDD* – тип DDoS-атаки; *NP* – количество пакетов, которое необходимо отправить на атакуемый узел; *f* – число пакетов, генерируемых в секунду, параметр *f* и *NP* определяют длительность атаки $T_{Attack} = NP / f$; $Sprt$ – сетевой порт, с которого отсылаются пакеты; Dad – адрес назначения (IP-адрес компьютера-жертвы); $Dprt$ – сетевой порт, на который отсылаются пакеты; *PS* – размер пакета; M_{spoof} – методики подмены сетевого адреса и порта. При выполнении DDoS-атак часто используются техники подмены IP-адреса отправителя. Более того, некоторые атаки основаны на подмене данного адреса.

Модели механизмов защиты. Множество базовых механизмов защиты представляются в виде $D = \langle TD, CD \rangle$, где TD – тип базового механизма защиты; CD – параметры механизма защиты, $CD \in \{n\}$.

Тип механизма защиты от инфраструктурных атак: $TD = \langle DWrm_{n,m}, DfDDoS_{n,m}, DAoR_{n,m}, DAoDNS_{n,m} \rangle$, где $DWrm_{n,m}$ – механизмы защиты от распространения сетевого червя; $DfDDoS_{n,m}$ – механизмы защиты от распределенных атак типа «отказ в обслуживании»; $DAoR_{n,m}$ – механизмы защиты от атак на маршрутизаторы; $DAoDNS_{n,m}$ – механизмы защиты от атак на DNS-сервера, переменная *n* служит для идентификации типа механизма защиты на верхнем уровне представления модели,

m определяет параметры заданного механизма защиты (например, место расположения механизма защиты в сети).

Рассмотрим теоретико-множественные модели базовых механизмов защиты от распространения компьютерного червя:

$DWrm_{n,m} \subseteq \langle DWrm' \rangle$, где $DWrm'$ множество подходов для защиты компьютерной сети от распространения сетевого червя.

$DWrm' = \langle TW, CW \rangle$, где TW – тип базового механизма защиты, CW – параметры механизма защиты.

В качестве базовых компонентов механизмов защиты от распространения червя можно выделить такие подходы, как дросселирование вирусов, анализ неудачных соединений и т.д. Тогда представим $DWrm_{n,m}$ как:

$DWrm_{n,m} = \{VT, FC, TRW, CB, ...\}$, где VT – механизм защиты на основе подхода «дросселирование вирусов» (Virus Throttling); *FC* – механизм защиты на основе подхода «анализ неудачных соединений» (Failed Connection); *TRW* – механизм защиты на основе подхода «случайного порогового прохождения» (Threshold Random Walk); *CB* – механизм ограничения интенсивности соединений на основе кредитов доверия (Credit Base-based Rate Limiting).

Представим модели механизмов защиты от DDoS-атак как:

$$DfDDoS_{n,m} = \{IEF, RBF, SV, HCF, SIM, SNd, MTP, SpA, KmT,$$

$$AcIn, HsBs, PMs, HIPF, SnK, SlPs, SOS, DWD, ...\},$$

где *IEF* – фильтрация входящего и исходящего трафика (Ingress/Edgress Filtering); *RBF* – фильтрация пакетов на маршрутизаторах (Router-Based Packet Filtering); *SV* – принудительная проверка адреса отправителя (Source Address Validity Enforcement, SAVE); *HCF* – фильтрация по количеству хопов (Hop-count filtering); *SIM* – мониторинг исходных IP адресов (Source IP Monitoring, SIM); *SNd* – обнаружение SYN-пакетов (SYN detection); *MTP* – MULTOPS; *SpA* – спектральный анализ (Spectral analysis); *KmT* – тест Колмогорова; *AcIn* – активное взаимодействие (Active Interaction); *HsBs* – трассировка на основе хешей (Hash-based traceback); *PMs* – вероятностные схемы маркировки пакетов (Probabilistic packet marking schemes); *HIPF* – фильтрация на основе истории полученных IP адресов (History-based IP Filtering); *SnK* – сброс полуоткрытых соединений (SYNkill); *SlPs* – Selective Pushback; *SOS* – использование оверлейных сетей (Secure overlay service); *DWD* – обнаружение аномалий на основе подхода D-WARD.

Подход «нервная система сети». Подход «нервная система сети» служит для объединения базовых подходов по защите сети от инфраструктурных атак и призван улучшить их эффективность. Подход базируется на распределенном механизме сбора и обработки информации для обнаружения атак и противодействия им. В каждой автономной системе имеется специальный сервер, который выполняет функции сбора и обработки информации, координации подключенных к нему узлов и обмена данными об атаках с серверами в других сетях. Узлы выполняют функции обнаружения и блокировки атак, а также передачи информации об обнаруженных атаках на сервер к которому они подключены.

Используем теоретико-множественное представление для определения модели «нервной системы сети». Представим «нервную систему сети» в виде $NN = \langle NS, NH \rangle$,

где NS – сервера «нервной системы сети»; NH – узлы нервной системы сети, например маршрутизаторы.

Сервер «нервной сети» содержит в себе следующие модули: $NS = \langle IM, PM, EM, CM, DM, sDB \rangle$, где IM – блок обмена данными с узлами «нервной сети»; EM – блок обмена данными между серверами «нервной системы сети»; DM – блок принятия решений и определения ответной реакции; sDB – база данных.

Рассмотрим более подробно блок принятия решений и определения ответной реакции: $DM = \langle PM, CM, dEE, dBE, dAD, F_{pm}, F_{cm}, F_{bkTr} \rangle$, где PM – модуль приоритезации полученных данных; CM – модуль корреляции полученных данных между собой; dEE – модуль обмена данными с другими серверами нервной системы сети и узлами локальной нервной системы сети; dBE – модуль обмена информацией с базой данных сервера; dAD – модуль принятия решений; F_{pm} – функция, описывающая работу модуля приоритезации; F_{cm} – функция, задающая работу модуля корреляции; F_{bkTr} – функция, определяющая функционирования модуля блокировки.

Представим узел «нервной сети» в следующем виде:

$NH = \langle AG, TR, NT, HD \rangle$, где AG – модуль сбора информации с сенсоров; TR – модуль обмена данными с сервером «нервной системы сети»; NT – модуль обмена данными между узлами «нервной системы сети»; HD – модуль, реализующий обработку трафика.

Подробнее остановимся на модуле обработки трафика: $HD = \langle RP, CP, VD, nDB, RA \rangle$, где RP – блок перенаправления потоков, выполняющий разделение трафика на потоки согласно адресу отправителя и адресу получателя; CP – блок классификации пакетов определяет протокол и тип пакеты (запрос на соединение, пакет с данными и т.п.); VD – блок анализа и противодействия; nDB – база данных узла; RA – блок сдерживания атак.

Для определения связей между компонентами «нервной системы сети» представим их в виде: $DE = \{Nd, P\}$, где Nd – взаимодействующие субъекты, P – тип связи.

Связь между серверами «нервной системы сети» определяется в виде: $DE_{S,S} = \{(S_{AS1}, S_{AS2}), IFSec3\}$, где S_{AS1} и S_{AS2} – сервера «нервной сети», между которыми установлена связь, $IFSec3$ – тип протокола, посредством которого осуществляется взаимодействие. Сервера обмениваются локальными «деревьями» или «глобальными деревьями» (задающими трассы вредоносной активности), необходимыми для построения маршрута прохождения вредоносного трафика от атакующего к атакуемому.

Связь между сервером и подчиненными ему узлами представляется в виде: $DE_{S,N} = \{(S_{AS1}, N_{AS1}^{\{1..n\}}), IFSec2\}$, где S_{AS1} и $N_{AS1}^{\{1..n\}}$ – сервера и узлы, между которыми установлена связь, $IFSec2$ – тип протокола, посредством которого осуществляется взаимодействие. Узлы передают данные серверам о детектированных атаках и получают команду на блокировку узлов.

Связь между узлами нервной сети внутри одной подсети представляется в виде: $DE_{N,N} = \{(N_{AS1}^{1}, N_{AS1}^{n}), IFSec1\}$, где N_{AS1}^{1} и N_{AS1}^{n} – узлы, между которыми установлена связь, $IFSec1$ – тип протокола, посредством которого осуществляется взаимодействие. Узлы нервной сети обмениваются данными об обнаруженных аномалиях, для детектирования вредоносных потоков.

Среда имитационного моделирования и эксперименты. Для реализации предлагаемого подхода, в качестве основного инструмента исследования, разрабатывается инструментальная среда для моделирования сетевых процессов в области инфор-

мационной безопасности. Архитектура среды задается в виде иерархии различных модулей и включает в себя систему моделирования дискретных событий, а также ряд компонентов, которые реализуют сущности более высокого уровня моделирования.

Нижний уровень среды моделирования *MS*, включает в себя планировщик *Sc*, посредством которого событиям *Ev* задается время вызова *T*. События оперируют сущностями *En*, которые обеспечивают взаимодействие множества элементов верхних уровней. Промежуточные уровни реализуют модели, характеризующие работу узлов в сети Интернет, например сетевые протоколы, типовые узлы и приложения. С их помощью осуществляется функционирование слоев более высокого уровня, определяющих механизмы атаки и защиты.

С использованием системы моделирования OMNeT++, библиотек INET Framework, ReaSE и собственных программных компонент предлагаемая архитектура была реализована для моделирования инфраструктурных атак и механизмов защиты от них.

Для оценки реализованных моделей инфраструктурных атак и механизмов защиты были проведены эксперименты. Проводились эксперименты по реализации таких атак, как распространение компьютерного червя и распределенная атака типа «отказ в обслуживании». В качестве механизмов защиты использовались модели на основе подходов Failed Connection, Virus Throttling, HCF, SIM, SAVE, SYN detection, а также подход «нервная система сети». Модели механизмов защиты имеют настраиваемые параметры, позволяющие производить поиск наиболее эффективных конфигураций.

Стратегии распространения сетевого червя оценивалось по проценту зараженных уязвимых компьютеров от общего количества уязвимых компьютеров. Выполнение атаки типа «распределенный отказ в обслуживании» оценивалось по количеству пакетов, приходящих на целевой узел в секунду. Качество работы механизмов защиты определялось по числу ошибок первого и второго рода, т.е. количеству ложных срабатываний (FP) и количеству пропущенных пакетов из атакующего трафика (FN).

Эксперименты показали, что в одинаковых условиях, комбинация механизма защиты «нервная система сети» и базовых механизмов защиты дает меньшее количество ложных срабатываний, позволяет серьезно снизить количество зараженных компьютеров в случае распространения сетевого червя и более эффективную фильтрацию атакующего трафика в случае выполнения атаки типа «распределенный отказ в обслуживании».

Заключение. На основе представленного теоретико-множественного подхода построены имитационные модели инфраструктурных атак на компьютерные сети и механизмов защиты от них, в том числе имитационная модель «нервной системы сети» и модель компьютерной сети, выполняющей роль среды взаимодействия стороны атаки и защиты. С помощью системы моделирования OMNeT++, библиотек INET Framework и ReaSE представленные модели использовались для создания среды имитационного моделирования атак на компьютерные сети и механизмов защиты от них. С помощью разработанной среды имитационного моделирования были проведены эксперименты по распространению сетевого червя, выполнения атак типа «распределенный отказ в обслуживании» и механизмов противодействия им.