Моделирование противоборства программных агентов в Интернете: общий подход, среда моделирования и эксперименты

И. В. Котенко, *д. т. н., профессор, руководитель научно-исследовательской группы компьютерной безопасности СПИИРАН*
ivkote@comsec.spb.ru
А. В. Уланов, *аспирант СПИИРАН*
ulanov@comsec.spb.ru

Вопросы моделирования процессов защиты информации активно исследуются на протяжении достаточно продолжительного периода времени. Создано большое количество разнообразных моделей отдельных механизмов защиты, но в недостаточной степени проработаны модели и методы, позволяющие формализовать комплексный антагонистический характер обеспечения информационной безопасности как сложного организационно-технического процесса. В работе предлагается подход к моделированию противоборства злоумышленников и систем защиты в сети Интернет в виде антагонистического взаимодействия команд программных агентов, представляющих злоумышленников и компоненты систем защиты. Предлагается использовать семейство различных моделей (от аналитических до полунатурных и натурных). Основное внимание уделяется применению агентно-ориентированного моделирования с использованием имитации процессов защиты информации на сетевом, транспортном и прикладном уровнях, что обеспечивает, с одной стороны, приемлемую для определенных классов задач точность процессов реализации компьютерных атак и механизмов защиты, а, с другой – их масштабируемость. Подход рассматривается на примере моделирования распределенных атак «отказ в обслуживании» и механизмов защиты от них.

Введение

В настоящее время мы является свидетелями все более возрастающей объективной зависимости всех сторон нашей жизнедеятельности от информационных технологий, в частности, от компьютерных технологий и открытых телекоммуникационных сетей, таких как Интернет. Без адекватного решения проблем безопасности этих технологий дальнейшее их использование становится невозможным.

Интернет постоянно находится под воздействием атак различных злоумышленников, зачастую достигающих своих целей. Текущее состояние противодействия систем нападения злоумышленников и систем защиты можно охарактеризовать как «*игру в сетевые кошки-мышки*» (a game of Network Cat and Mouse) – кто кого обманет [1].

Злоумышленники (кибертеррористы)-профессионалы для достижения своих целей в киберсреде способны реализовать развитые *стратегии осуществления различных угроз безопасности*, которые могут включать комплекс различных действий:

- сбор информации о системе, обнаружение уязвимостей и используемых средств защиты (в том числе механизмов аутентификации, раз-

граничения доступа, обнаружения вторжений и др.);
- моделирование способов преодоления защиты (на своем рабочем месте, стенде моделирования, тестовом полигоне);
- подавление средств защиты, их обход или обман (например, посредством реализации «растянутого» во времени скрытого сканирования, выполнения отдельных скоординированных действий (атак) из нескольких различных источников, вместе составляющих сложную многофазную атаку и др.);
- использование уязвимостей и получение доступа к ресурсам, повышение полномочий, реализацию своей цели;
- скрытие следов своей деятельности и создание «черных ходов» для использования их для последующего вторжения.

Поэтому обеспечение информационной безопасности в современных условиях требует выполнения в реальном времени непрерывного комплекса разнообразных мероприятий:
- реализации механизмов защиты, соответствующих установленной политике безопасности (в том числе проактивного предупреждения атак и препятствования их выполнению, дезинформации злоумышленника, сокрытия и камуфляжа важных ресурсов и процессов);
- сбора информации о состоянии информационной системы и анализа обстановки за счет механизмов обработки информации из различных источников;
- обнаружения аномальной активности, нелегитимных действий, атак и вторжений;
- предсказания намерений и возможных действий злоумышленников;
- непосредственного реагирования на вторжения, в том числе введения злоумышленника в заблуждение, заманивания злоумышленника с использованием ложных компонентов с целью раскрытия и уточнения его целей;
- рефлексивного управления поведением злоумышленника, усиления критических механизмов защиты;
- устранения последствий вторжения, обнаруженных уязвимостей и адаптации системы обеспечения информационной безопасности к последующим вторжениям.

К сожалению, существующая теоретическая база для обеспечения информационной безопасности в крупномасштабных системах (таких, как Интеренет) не предоставляет возможности адекватно формализовать указанный комплекс процессов. На наш взгляд, в первую очередь, это обусловлено недостаточным вниманием к исследованиям, которые, с одной стороны, рассматривают задачу обеспечения информационной безопасности как *комплексную задачу организационного и технического компьютерного противоборства* между системами защиты информации и системами компьютерного нападения злоумышленников, а, с другой – базируются на исследовательском моделировании указанного комплекса процессов.

Хотя исследователи в состоянии представить отдельные механизмы защиты, понимание системы обеспечения информационной безопасности как *единой (холической) системы*, зависящее от учета множества взаимодействий между отдельными процессами ее функционирования и киберпротивостояния между различными элементами, а также развивающегося динамического характера этих процессов и отдельных компонентов информационных систем, чрезвычайно затруднено. Особенно это справедливо с учетом наблюдаемой в настоящее время *эволюции Интернет в свободную децентрализованную распределенную среду взаимодействия огромного числа кооперирующихся и антагонистических программных агентов.*

Проблема защиты от атак типа «Распределенный отказ в обслуживании»

Рассмотрим указанную выше проблему на примере исследования и реализации механизмов защиты от одного из наиболее критичных по последствиям классов компьютерных атак – «Распределенный отказ в обслуживании».

В результате известной атаки *«отказ в обслуживании»* (Denial of Service, DoS), сводящейся, как правило, к передаче большого количества сетевых пакетов с одного их хостов сети (хотя существуют и другие виды атак DoS), законный пользователь не может получить доступ к необходимой ему информации. Большинство операционных систем, маршрутизаторов и других компонентов сетей подвержены атакам DoS, предотвратить которые очень сложно. В начале 2000 года появился новый класс атак – *«распределенный отказ в обслуживании» (Distributed Denial of Service, DDoS)* [2]. Для проведения данной атаки злоумышленник должен сначала скомпрометировать большое количество компьютеров для запуска на них средств DoS и последующего одновременного нападения на некоторый компьютер или сеть. Это существенно усложняет как обнаружение, так и защиту от атак данного класса.

Известно множество различных видов атак DDoS. Условно их можно разделить на две категории: истощение ресурсов сети и истощение ресурсов хоста. Атаки осуществляются с помощью непосредственной посылки жертве большого количества пакетов (как, например, UDP и ICMP flood) или использования для этой цели промежуточных узлов (примеры: Smurf и Fraggle), передачи слишком длинных пакетов (Ping Of Death), некорректных пакетов (Land) или большого количества трудоемких запросов (TCP SYN) и др.

Построение эффективной системы защиты от атак DDoS является сложной задачей: она должна включать в себя механизмы предупреждения атаки, обнаружения факта атаки, определения источника атаки и противодействия атаке.

Стандартной мерой защиты подсети (не только от атак DDoS) является установка правил фильтрации пакетов от зарезервированных IP-адресов (например, для сетевых пакетов, входящих с адресами из внутренней подсети, выходящих с адресами, отличающимися от внутренних, необычных по размеру; к тем и от тех портов, которые не задействованы в системе, по неиспользуе-

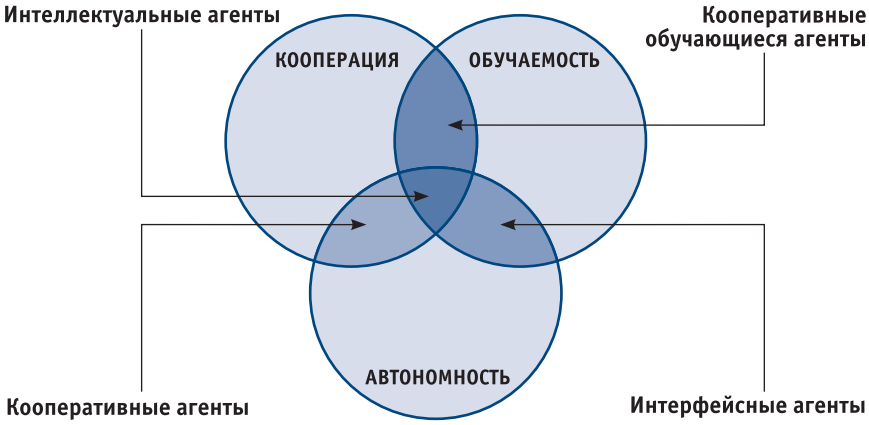

Рис. 1. ***Представление основных свойств агента***

мым протоколам и др.). Кроме того, применяется ограничение на трафик для каждого протокола для входящих/выходящих потоков и множество других мер. Зная о них, злоумышленник может таким образом модифицировать параметры атаки DDoS (например, на основе изменения IP-адреса отправителя), что ее будет невозможно отличить от запросов пользователей, вызванных, например, повышенным интересом к данному серверу. Это требует существенного усложнения механизмов защиты.

Разработать адекватные методы защиты от атак DDoS и выработать обоснованные рекомендации по выбору механизмов защиты, наиболее действенных в конкретных условиях, можно, используя исследовательское моделирование атак DDoS и механизмов защиты от них.

Формализация, моделирование и исследование противоборства злоумышленников и систем защиты в сети Интернет на примере моделирования процессов реализации распределенных атак «отказ в обслуживании» и механизмов защиты может позволить получить результаты, обобщаемые на другие задачи, в частности, на задачи информационной борьбы в Интернете, конкуренции в сфере электронного бизнеса и др. [3].

Подход к моделированию кибернетического противоборства

Определим, что мы будем понимать под термином интеллектуальный агент. *Интеллектуальный агент* – это программно или аппаратно реализованная система, обладающая автономностью, возможностью принимать решения по способу своего функционирования и способная выполнять свои функции в сообществе с другими агентами. Основные свойства агента представлены на рис. 1 [4]. Агенты, которые прилагают совместные усилия для достижения общей долговременной цели, функционируют в динамической внешней среде в условиях противодействия со стороны соперника, образуют *команду агентов*. В состав команды агентов входит множество интеллектуальных агентов, взаимодействующих друг с другом и внешней средой.

Использование основанного на многоагентных технологиях моделирования процессов обеспечения информационной безопасности в сети Интернет предполагает, что *кибернетическое противоборство представляется в виде взаимодействия различных команд программных агентов*. Агрегированное поведение системы проявляется посредством локальных взаимодействий отдельных агентов в динамической среде, задаваемой посредством модели компьютерной сети.

Выделяется две команды агентов, воздействующих на компьютерную сеть, а также друг на друга: команда агентов-злоумышленников по реализации атак DDoS и команда агентов защиты.

Задача многоагентного моделирования процессов кибернетического противоборства представляется как моделирование антагонистического взаимодействия, по крайней мере, одной команды агентов-злоумышленников и одной команды агентов защиты.

Цель команды агентов-злоумышленников заключается в определении уязвимостей компьютерной сети и системы защиты и реализации заданного перечня угроз информационной безопасности посредством выполнения распределенных скоординированных атак. Цель команды агентов защиты состоит в защите сети и собственных компонентов от атак.

Агенты различных команд *соперничают* для достижения противоположных намерений. Агенты одной команды *сотрудничают* для осуществления общего намерения (по реализации угрозы или по защите компьютерной сети).

Предполагается, что соперничающие агенты осуществляют сбор информации из различных источников, оперируют нечеткими (вероятностными) знаниями, прогнозируют намерения и действия оппонента, реагируют на его действия, оценивают возможные риски, пытаются обмануть друг друга.

Выбор сценария поведения каждой из команд зависит, прежде всего, от выбранной цели функционирования, а конкретная реализация сценария определяется, в первую очередь, непосредственной реакцией противоположной команды. Поэтому выбор каждого очередного шага поведения каждой из команд должен определяться динамически в зависимости от действий противоположной команды и состояния среды.

Каждая команда действует *в условиях ограниченной информации*, а каждый ее член может обладать различной информацией о действиях других членов команды. Поэтому модель поведения агентов должна быть в состоянии отображать неполноту информации и возможность возникновения случайных факторов. Кроме того, само поведение агентов должно зависеть от информации, которой владеет команда, и от ее распределения на множестве отдельных агентов, входящих в состав команды [3].

Модели функционирования агентов предусматривают, что каждый

агент «знает», какие задачи он должен решать сам и к какому агенту он должен адресовать свой запрос на информацию или на решение подзадачи с целью получения такой информации, если это вне его компетенции. Сообщения одних агентов представляются в форме и терминах, понятных другим агентам [5]. Одним из наиболее перспективных подходов к структуризации распределенных баз знаний такого типа является использование *онтологий*, характеризующих предметные знания сами по себе, вне связи с конкретными структурами их представления, алгоритмами вывода или эвристиками [5, 6]. Как и для любой другой предметной области, онтология области защиты информации представляет собой описание частично упорядоченного множества понятий, которые должны использоваться соответствующими агентами. Кроме отношений частичного порядка, на узлы этой структуры накладываются и другие отношения, свойственные предметной области. Это различного рода ограничения, правила, количественные и качественные отношения, связывающие понятия рассматриваемой предметной области. Данная онтология определяет подмножество понятий, которые используют различные агенты для кооперативного решения поставленных задач. Каждый агент использует определенный фрагмент общей онтологии предметной области.

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).

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 исполняемой политики безопасности, формирования новых экземпляров механизмов и профилей защиты.

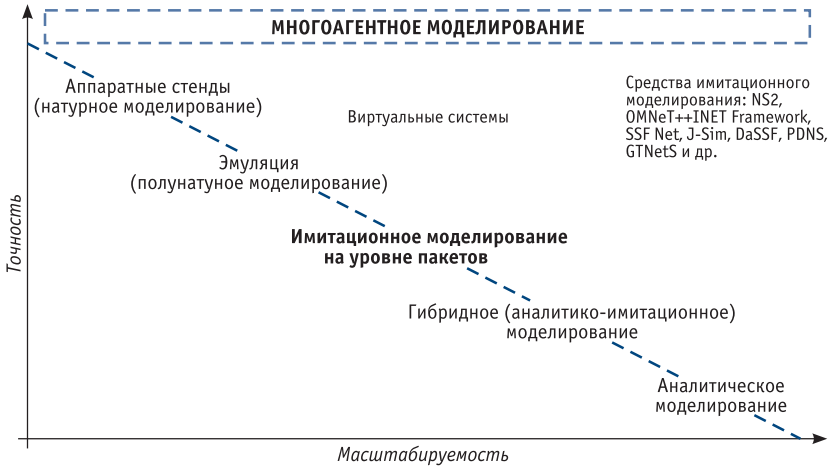

Рис. 2. ***Семейство моделей, используемых для исследовательского моделирования компьютерного противоборства***

Взаимодействие между агентами может быть представлено как игра двух соперников, в которой целью агентов является поиск стратегии, которая максимизирует ожидаемый интегральный выигрыш в игре [7–9].

Стратегии функционирования агентов могут быть представлены посредством различных формализмов, например, на основе семейства стохастических атрибутных формальных грамматик (и их интерпретации с использованием автоматов) и скрытых марковских моделей.

Концептуальная модель кибернетического противоборства включает в себя:

- онтологию приложения в области защиты информации, содержащую множество понятий приложения и отношений между ними;
- протоколы командной работы агентов различных команд (команд злоумышленников и команд (компонентов) системы защиты информации);
- модели сценарного индивидуального, группового и общекомандного поведения агентов в рамках конкретных намерений, реализуемых сценариями;
- коммуникационный компонент, предназначенный для обмена сообщениями между агентами;
- модели среды функционирования – компьютерной сети, включающие топологический и функциональные компоненты.

Предлагаемая технология создания команды агентов заключается в реализации следующей цепочки этапов [10]:

- формировании онтологии предметной области;
- определении структуры команды агентов и механизмов их взаимодействия и координации (в том числе задание ролей и сценариев обмена ролями между агентами);
- спецификации иерархии планов действий (генерации атак);
- назначении ролей и распределения планов между агентами.

Для исследовательского моделирования процессов кибернетического противоборства предлагается использовать семейство различных моделей (от аналитических до полунатурных и натурных) (рис. 2) [11].

Выбор конкретных моделей определяется необходимой точностью и масштабируемостью моделирования. Например, аналитические модели позволяют имитировать глобальные процессы, происходящие в Интернете (в том числе вирусные эпидемии), однако эти модели описывают моделируемые процессы только на абстрактном уровне. Имитационное моделирование на уровне пакетов предоставляет возможность до-

статочно адекватно воспроизводить протекающие процессы, представляя атакующие и защитные действия с помощью обмена сетевыми пакетами, точно имитируя работу по протоколам канального, сетевого, транспортного и прикладного уровней. Наибольшая точность имитации достигается на аппаратных стендах при натурном моделировании, однако при этом удается моделировать достаточно ограниченные фрагменты взаимодействий агентов.

Основное внимание в настоящей работе уделяется применению имитационного моделирования на уровне пакетов с использованием в качестве базового уровня среды моделирования соответствующих средств имитационного моделирования, позволяющих имитировать сетевые процессы.

Организация командной работы агентов: релевантные работы и сущность подхода

В качестве начального фундамента для исследований в области моделирования противоборства злоумышленников и систем защиты в сети Интернет, используются работы в следующих областях: агентно-ориентированное моделирование; командная работа агентов; системы вывода, основанные на предсказании намерений и планов оппонента; рефлексивные процессы; теоретико-игровое моделирование; моделирование атак на компьютерные сети; моделирование механизмов защиты информации; адаптивные системы и эволюционные вычисления.

Методы агентно-ориентированного моделирования являются сравнительно молодой областью применения теории многоагентных систем, поэтому решение поставленной проблемы должно привести, в том числе, и к обогащению этого направления.

Основной базис для исследования составляет теория командной работы агентов. Известно три классических подхода к формализации командной работы агентов.

В *теории общих намерений* [12] команда агентов имеет общую долговременную цель. Все члены команды хотят, чтобы эта цель была достигнута. Агенты обладают индивидуальными обязательствами, которые являются их долговременной целью. Индивидуальные намерения агентов заключаются в выполнении этой цели. Аналогично, команда агентов имеет общие обязательства и намерения. Команда агентов имеет общее намерение выполнить некоторое действие, если все члены команды имеют общую долговременную цель выполнить это действие. О том, достигнута ли цель, агенты должны прийти к соглашению. При выполнении командой последовательности действий, каждый агент должен иметь индивидуальное намерение и исполнять его как часть общего намерения. Во время командных действий план может многократно меняться.

Согласно *теории общих планов* [13] под групповым планом понимается план совместного выполнения некоторого множества действий группой агентов. Групповой план действий требует, чтобы команда агентов пришла к соглашению по выполнению предписаний, которым они будут следовать в групповых действиях. Агенты должны принять на себя обязательства по отношению не только к своим индивидуальным действиям, но также и по отношению к действиям группы в целом. Аналогично, агент должен принять на себя обязательства по отношению к действиям других агентов. План групповой деятельности может иметь в качестве отдельных компонентов как планы индивидуальных агентов для назначенных действий, так и планы подгрупп.

Модель командной работы агентов, предложенная в работе [14], основана на *комбинировании теорий общих намерений и общих планов* и пытается использовать преимущества каждой. Эта модель реализована в системе STEAM. Общие намерения агентов отображены в иерархическом реактивном плане, в котором описываются как действия команды в целом, так и отдельных агентов. Согласованные задачи выполняются благодаря установке ограничений на роли агентов (на их поведение). Теория общих планов предоставляет необходимые механизмы решения этой задачи. Кроме того, процесс достижения цели отслеживается агентами.

Многие подходы к организации командной работы агентов воплощены в программных реализациях различных многоагентных систем, например, в системах GRATE*, OAA, CAST, RETSINA-MAS, COGNET/BATON, Team-Soar и др. Важным полигоном для исследования командной работы агентов является «виртуальный футбол» (футбол роботов) и моделирование спасательных действий команд агентов в различных критических ситуациях (при стихийных бедствиях, террористических актах и т. п.).

Система GRATE* [15] является реализацией модели командной работы с общей ответственностью (Joint Responsibility). Она включает в себя понятия общих целей (из теории общих намерений) и общих предписаний. То, как агент должен действовать для решения задачи в контексте совместной работы, определяется индивидуальными обязательствами по предписанию (Individual recipe commitment). Общие обязательства по предписанию обязывают агента в случае невыполнения им обязательств пытаться сообщить об этом всем агентам команды. Общая ответственность подразумевает, что агенты имеют общую долговременную цель, выполняют общие обязательства по предписанию и им известно о действиях друг друга.

В основу «открытой агентской архитектуры» (Open Agent Architecture, OAA) [16] положены понятия «доски объявлений» (blackboard) и «ассистента» (facilitator). «Доска объявлений» является глобальным хранилищем. Агенты могут общаться через это хранилище: считывать, записывать, запрашивать данные. Ассистенты гарантируют прозрачность выполнения запросов, управляют составными целями и заведуют размещениями данных и триггеров. Триггеры – это механизмы, которые должны сработать, если достигнуты заданные условия. С их помощью организуется скоординированная работа агентов.

Основная идея системы CAST [17] заключается в использовании общей ментальной модели агентов для проактивного обмена информацией в целях эффективного командного поведения. Общая ментальная модель состоит из общих знаний, убеждений о мире и убеждений о взаимной ответственности членов команды (они зафиксированы в виде сети предикатов). Для принятия решения о том, какие действия должен выполнить агент на следующем шаге, используются специальные алгоритмы. Исходя из ограничений, указанных в плане, выбираются агенты, необходимые для выполнения поставленной задачи. С этой же целью затем определяются наилучшие моменты для проактивной передачи информации.

В модели командной работы RETSINA-MAS [18] предполагается, что у всех агентов есть своя собственная копия частичного плана для выполнения цели. Каждый агент оценивает свои возможности по выполнению условий задачи и составляет набор ролей. Агенты сопоставляют возможные роли, пока они не покроют все требования без возникновения конфликтов. После этого они приступают к выполнению командного плана. Координация агентов осуществляется на основе их ролей с помощью определения их возможностей.

Система COGNET/BATON [19] предназначена для моделирования командной работы людей с использованием интеллектуальных агентов. Для осуществления командной работы используется «доска объявлений», которая есть у каждого агента. На ней он отображает состояние других членов команды и отношение его локальных действий к долговременным целям команды. Эффективные командные действия обеспечиваются тем, что агентам необходимо периодически совместно составлять собственные «доски объявлений». Для описания деятельности команды используются деревья целей.

Система Team-Soar [19] предназначена для проверки теории командного принятия решения под названием «multilevel theory».

В «виртуальном футболе» (Robocup Soccer) [20] агенты имеют общие правила и знания, которые управляют их кооперативным поведением. Агенты действуют, ориентируясь на собственную модель мира, куда входят, в том числе, и убеждения о действиях других агентов.

Еще одной фундаментальной составляющей проводимых исследований являются работы в области *систем вывода, основанных на знаниях о выполняемых действиях и предсказании намерений и планов оппонента* на основе оценки текущей ситуации. Наряду со ставшими уже классическими работами Е. Чарниака [21], сформулировавшего задачу распознавания как задачу абдуктивного вывода, Х. Каутца и Д. Алена [22], рассматривающих распознавание плана на основе идентификации минимального множества высокоуровневых действий, которые достаточны для объяснения наблюдаемых событий, М. Вилейна [23], использующего для распознавания методы грамматического анализа, М. Веллмана и Д. Пинадаса [24], предложивших механизмы байесовского распознавания, и др., сравнительно недавно были опубликованы работы по определению планов злоумышленников при обнаружении вторжений, в частности, работы К. Гейба и Р. Голдмана [25, 26]. Предполагается использовать идеи распознавания планов действий агентов на основе алгоритмов восстановления стохастических формальных грамматик, изученных авторами настоящей статьи в результате предыдущих исследований [27].

Важной компонентой, необходимой для использования в работе, являются методы *теории рефлексивных процессов* [28–30 и др.], *теоретико-игрового информационного моделирования* [7–9, 31 и др.] и *управления в конфликтных ситуациях* [32 и др.].

Используемые авторами методы спецификации сценариев действий агентов, основанные на стохастических атрибутных формальных грамматиках [33], можно соотнести с развиваемой в настоящее время *теорией построения систем (колоний) кооперативных распределенных грамматик* и грамматическими моделями многоагентных систем [34–37].

Команды агентов атаки и защиты должны адаптироваться к реконфигурации аппаратного и программного обеспечения сети, к изменению трафика, а также к новым видам защиты и атакам на основе прошлого опыта и алгоритмов. Следовательно, важно учитывать существующие исследования в области *адаптации и самообучения агентов* [38–44 и др.].

Предлагаемый в настоящей работе подход к организации командной работы агентов базируется на совместном использовании элементов теории общих намерений, теории разделяемых планов и комбинированных подходов и учитывает опыт программной реализации ряда многоагентных систем [45, 46].

Предполагается, что командная работа агентов организуется с помощью *общего (группового) плана действий*, особенности которого заключаются в следующем [47] (рис. 3):

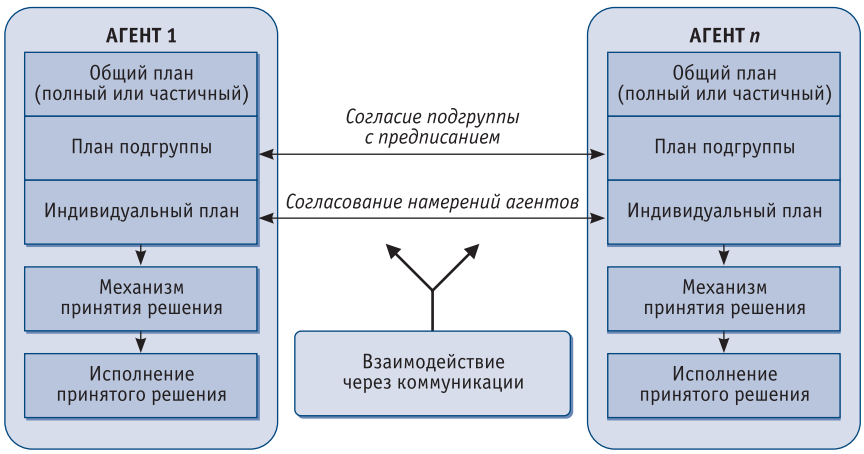

Рис. 3. ***Схема реализации командной работы агентов***

- групповой план действий требует, чтобы команда агентов пришла к согласию выполнять предписание (множество заданных инструкций);
- агенты должны принять на себя обязательства по отношению не только к своим индивидуальным действиям, но также к действиям других агентов и действиям группы в целом;
- план групповой деятельности может иметь в качестве компонентов как планы индивидуальных агентов для назначенных действий, так и планы подгрупп;
- при выполнении командной работы агенты команды должны с помощью коммуникаций прийти к согласию с предписанием, а также согласовать собственные намерения друг с другом.

Структура команды агентов описывается в терминах иерархии групповых и индивидуальных ролей. Конечные узлы иерархии отвечают ролям индивидуальных агентов, промежуточные узлы – групповым ролям.

Спецификация иерархии планов действий осуществляется для каждой из ролей. Для каждого плана задаются:

- 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.

У членов команды – общая ментальная модель. Агенты могут строить «срезы» ментального состояния команды в целом с помощью формирования общих намерений на разных уровнях абстракции. Иерархия намерений устанавливается совместно членами команды, чтобы команда выполняла цели согласованно. Это – следствие установления агентами обязательств друг перед другом.

Механизмы координации и взаимодействия агентов базируются на трех группах процедур [14, 46]:

- обеспечении согласованности действий;
- мониторинге и восстановлении функциональности агентов;
- обеспечении селективности коммуникаций (для выбора наиболее «полезных» коммуникационных актов).

Процедуры обеспечения согласованности действий агентов необходимы для поддержки скоординированной деятельности последних по некоторому сценарию. Эти процедуры реализуются путем обмена агентами информацией о результатах деятельности, которые непосредственно влияют на выполнение поставленной задачи. До начала реализации атаки DDoS происходит формирование необходимого количества агентов, до их сведения доводятся их роли. Далее агенты сообщают о своей готовности и начинают активные действия в соответствии с заданной ролью. При достижении поставленной цели, обнаружении невозможности выполнить цель или выявлении нерелевантности цели агент обязан сообщить этот факт оставшимся членам команды. При этих условиях выполняемый сценарий завершается, и должен быть активизирован другой сценарий.

Процедуры мониторинга и восстановления функциональности агентов направлены на сохранение работоспособности и функциональности команды агентов. Их реализация может происходить с использованием различных приемов, например, за счет перераспределения ролей среди оставшихся агентов взамен выбывших или путем генерации новых агентов с соответствующей ролью и функциональностью, если количество работоспособных агентов достигло критического числа.

Процедуры обеспечения селективности коммуникаций служат для минимизации количества коммуникативных актов с целью уменьшения вероятности раскрытия агентов и сокращения используемых ресурсов. Эти процедуры реализуются на основании знаний о выгоде коммуникационного акта и «затратах» на его обеспечение.

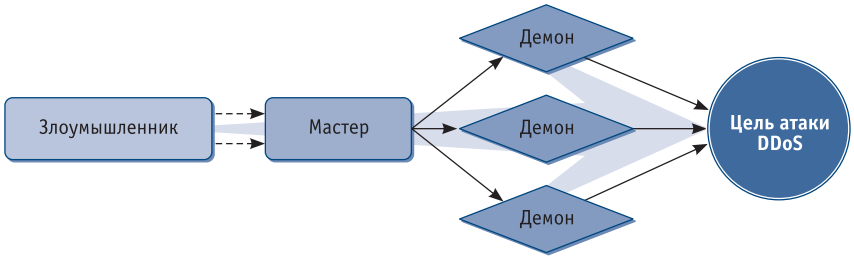

Рис. 4. ***Двухуровневая структура команды агентов атаки***

Структура команд агентов атаки и защиты

Команда атаки

Глобальная цель атаки DDoS – «отказ в обслуживании» некоторого ресурса – достигается совместными усилиями многих компонентов, действующих на стороне атаки. Таким образом, исходная задача разбивается на более простые, которые поручаются отдельным специализированным компонентам. При этом на верхнем уровне цель остается общей для всех компонентов. На нижнем уровне формируются локальные цели, достижение которых направлено на решение общей задачи. Компоненты взаимодействуют между собой для координации локальных решений, что необходимо для достижения требуемого качества выполнения общей цели «отказ в обслуживании». В случае, если управление атакой осуществляется злоумышленником-человеком, выделяется отдельный компонент для координации работы непосредственных участников атаки со стороны злоумышленника.

Компоненты системы DDoS-атаки являются, как правило, программами. Они обладают следующими свойствами:

- автономностью;
- наличием исходных знаний о себе, взаимодействующих сущностях и внешней среде, заданных разработчиком;
- наличием знаний или жесткого алгоритма, позволяющего получать и обрабатывать внешние данные из среды;
- наличием цели и списка действий для достижения этой цели;

- осуществлением коммуникации и взаимодействия для достижения общей цели.

Эти свойства позволяют представить каждый компонент системы атаки интеллектуальным агентом, а их набор – командой агентов.

Представим систему атаки DDoS в виде команды агентов [48]. Агенты преследуют общую цель – проведение атаки «отказ в обслуживании» на некоторый узел или сеть.

Анализируя существующие способы реализации атак DDoS, можно определить два *основных типа компонентов системы атаки*:

- «демон» – агент, непосредственно выполняющий атаку DoS,
- «мастер» – агент, выполняющий действия по координации остальных компонентов системы.

Структура команды изображена на рис. 4.

На предварительном этапе демоны и мастер устанавливаются на доступные (скомпрометированные) узлы сети Интернет. Здесь важными параметрами являются количество и распределенность агентов. Затем происходит организация команды атаки: демоны посылают мастеру сообщения о том, что они существуют и готовы к работе мастер хранит информацию о членах команды и об их состоянии.

Злоумышленник задает общую цель команды – совершить атаку DDoS. Параметры атаки получает мастер. Его цель – разослать их всем доступным демонам. Далее в действие вступают демоны. Их локальная цель – исполнить команду мастера. Для этого на указанный узел отсылаются пакеты атаки. После этого считается, что цель команды на данном этапе достигнута.

Периодически мастер опрашивает демонов, для того, чтобы узнать о том, что они находятся в работоспособном состоянии. Получая сообщения от демонов, мастер контролирует заданный режим выполнения атаки. Если от какого-либо демона не поступает сообщений о состоянии, мастер принимает решение об изменении параметров атаки, например, посылая команды всем или только определенным демонам об изменении интенсивности атаки.

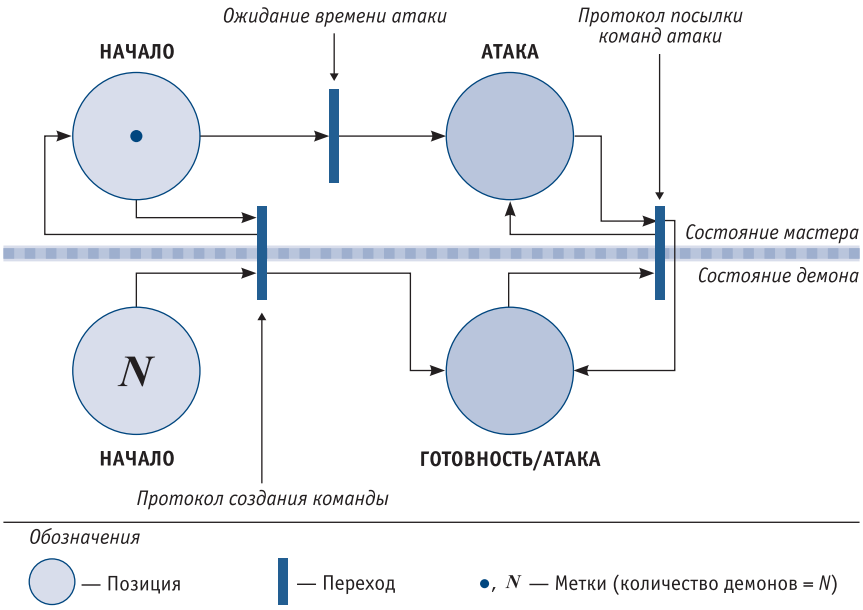

Рис. 5. ***Командная работа агентов атаки***

Демоны могут выполнять атаку в различных режимах. Это влияет на возможности команды защиты по обнаружению и блокированию атаки, а также отслеживанию и устранению агентов атаки. Демоны могут отправлять пакеты атаки с различной интенсивностью, подменять адрес отправителя и делать это с различной частотой.

Злоумышленник может прекратить атаку. Он задает мастеру команду «завершить атаку». Затем мастер рассылает соответствующие команды демонам. Получив ее, демоны прекращают атаку.

Совместное поведение членов команды можно представить с помощью сети Петри (рис. 5). Кружками обозначены позиции сети. Это – состояния агентов. Текущее состояние содержит метку – точку (если метка одна) или число меток. Перейти из одного состояния в другое агент может с помощью перехода, обозначенного черными прямоугольниками. Переход осуществляется по дугам в направлении стрелок. Переход может сработать, если в каждой его исходной позиции количество меток не меньше, чем количество дуг. При переходе это количество вычитается из количества меток в исходной позиции. При этом на переход может быть наложены условия, например, достижение некоторого результата во входной позиции (состоянии).

Команда защиты

Анализ существующих систем защиты от атак DDoS позволил выявить следующие их особенности:

- системы защиты строятся из базовых компонентов, каждый из которых имеет определенное локальное назначение, но служит общей задаче;
- набор и функциональность компонентов системы защиты зависит от места установки системы;
- системы защиты имеют несколько уровней, на которых решаются отдельные подзадачи комплексной задачи защиты.

Общий подход к защите от атак DDoS заключается в следующем. Осуществляется сбор информации о нормальном для данной сети трафике с помощью сенсоров. Затем компонентом-анализатором в режиме реального времени осуществляется обнаружение атак на основе сравнения текущего трафика с модельным. С помощью механизмов трассировки (traceback) система пытается проследить источник аномалий и выдает рекомендации по их отсечению или снижению их количества. В зависимости от выбора администратора безопасности (пользователя системы) системой применяется та или иная контрмера.

Механизмы обнаружения атак DDoS можно классифицировать по месту расположения и по способу обнаружения. Компоненты обнару-

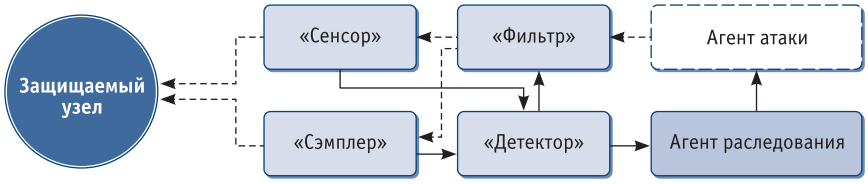

Рис. 6. ***Обобщенная структура команды агентов защиты***

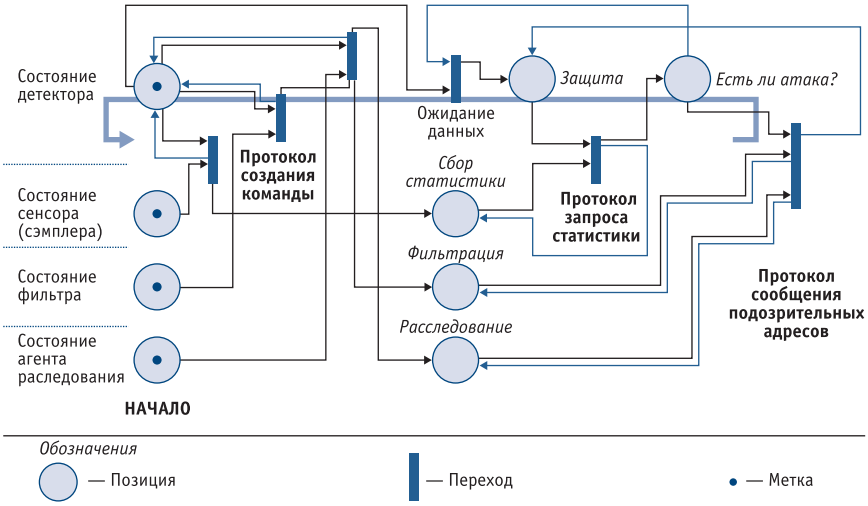

Рис. 7. ***Командная работа агентов защиты***

жения могут располагаться в атакуемой сети, в исходной или промежуточной подсетях. Модель нормального для данной сети трафика строится на основе доступных данных: либо явно, либо после обработки на базе какого-либо метода. Эта модель строится, как правило, по нагрузке, по сигнатуре, по статистике, с использованием традиционных статистических и других методов.

Механизмы противодействия атакам DDoS можно классифицировать, как и механизмы обнаружения, учитывая место расположения и применяемый способ защиты. Место расположения определяется тем, для защиты какой подсети установлена данная система. Это может быть подсеть цели атаки, исходная или промежуточная подсеть. Эффективно построенная система противодействия фрагмента сети, кроме собственной защиты, положительно влияет также и на защиту сети в целом, например, блокируя внутри себя пакеты атаки.

Способы защиты могут быть следующими:

- фильтрация пакетов (используется в большинстве случаев);
- фильтрация потоков, изменение количества ресурсов;
- перенос ресурсов;
- разграничение ресурсов;
- аутентификация и др.

Дополнительно можно выделить три варианта применения фильтрации. Первый вариант – это стандартная фильтрация, выполняемая на одном хосте. Второй – с отражением (pushback), когда фильтр применяется на каждой итерации все ближе к источнику атаки. Третий – с отслеживанием (traceback), когда источник атаки отслеживается, и фильтр применяется на ближайшем к нему хосте (маршрутизаторе).

Представим *систему защиты от атак DDoS* в виде команды интеллектуальных агентов [48]. Они преследуют общую цель, заключающуюся в защите заданного узла или сети от атаки DDoS.

В соответствии с общим подходом, зададим следующие классы агентов защиты:

- первичной обработки информации («сенсор»);
- сбора данных для формирования модели трафика сети («сэмплер»);
- обнаружения («детектор»);
- фильтрации («фильтр»);
- расследования.

На рис. 6. представлена обобщенная структура команды защиты и взаимодействия агентов защиты с агентами атаки.

Дополнительно можно выделить еще один класс агентов – агентов управления («менеджеров»), которые служат для взаимодействия с администратором безопасности и конфигурирования системы защиты.

Общая цель команды агентов защиты – противостояние атаке DDoS. За ее выполнением следит детектор.

Команда агентов состоит из заданного числа сенсоров. *Агенты-сенсоры* расположены в определенных местах сети, откуда они осуществляют мониторинг сетевых процессов с целью сбора статистических данных. Сенсоры определяют величину всего трафика (бит в секунду (bit per second) – BPS), а также адреса n узлов, создающих наибольший трафик . Их локальная цель – предоставлять эти данные каждые k секунд агентам детектирования для выявления аномалий и возможности атаки DDoS.

Сэмплеры обрабатывают информацию о сетевых пакетах и на ее основе составляют модель нормального для данной сети трафика (в режиме обучения). Затем, в нормальном режиме, они анализируют сетевой трафик на соответствие модельному и выделяют IP-адреса нарушителей, которые затем отсылаются детекторам. Для обнаружения атаки используются методы Hop counts Filtering (HCF) [49], Source IP address monitoring (SIPM) [50], Bit Per Second (BPS) и др.

Агенты обнаружения принимают решение, есть ли опасность атаки DDoS, и от каких узлов она может исходить. Они передают эту информацию агентам расследования и (или) фильтрации.

Агенты фильтрации устанавливаются на пути прохождения сетевых пакетов к защищаемому узлу или сети и могут использовать различные механизмы фильтрации злонамеренных сетевых пакетов.

Агенты расследования пытаются проследить источники атак DDoS и обезвредить таковые путем вывода из строя соответствующих агентов атаки.

Совместное поведение членов команд защиты и атаки можно представить с помощью сети Петри (рис. 7).

Окончание в следующем номере.