УДК 004.896

ПРИМЕНЕНИЕ ИНТЕЛЛЕКТУАЛЬНЫХ МУЛЬТИАГЕНТНЫХ ТЕХНОЛОГИЙ ДЛЯ МОДЕЛИРОВАНИЯ РАСПРОСТРАНЕНИЯ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В ГЕТЕРОГЕННЫХ КОМПЬЮТЕРНЫХ СЕТЯХ

Чумаченко Дмитрий Игоревич, доцент кафедры информатики
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»

Широкое использование и легкий доступ к сети Интернет делает его главной мишенью для злонамеренной деятельности. В частности, Интернет стал мощным механизмом для распространения вредоносного программного обеспечения. Сетевые черви, автономные программы, распространяющиеся через компьютерные сети при помощи автоматического поиска, атак и заражения удаленных компьютеров, разрабатываются практически 30 лет с момента первого червя Морриса. В современных условиях, компьютерная инфраструктура более уязвима, чем когда-либо ранее, т.к. скорость развития технологий намного выше скорости разработки их защитных мер.

Разработка точной модели Интернет-червя даст представление о его поведении. Это позволит выявить слабые места в динамике сетевого червя, а также создать прогноз его распространения с целью оценки ущерба от деятельности червя. В эпидемиологических исследованиях, существует несколько детерминированных и стохастических моделей для распространения вирусных заболеваний, также, некоторые модели существуют и для моделирования распространения Интернет-червей, однако они не позволяют учитывать динамический характер развития эпидемического процесса вредоносного программного обеспечения.

В рамках данного исследования разработана мультиагентная модель распространения сетевого червя на примере червя Code Red, которая позволяет устранить недостатки детерминированных аналитических моделей.

Адекватность мультиагентной модели в большой степени зависит от количества агентов в системе. Использование больших популяций и детализация свойств агентов приводит к необходимости применения наиболее современных информационных средств и технологий, в частности – алгоритмов, оптимальных по количеству выполняемых машинных операций. При мультиагентном подходе процесс моделирования основывается на построении и обработке очереди событий, которые можно разделить на два типа:

1. Изменение состояния агента с точки зрения внешней среды (физическое положение агента);

2. Изменение внутреннего состояния агента. События этого типа возникают в результате взаимодействия агента с другими агентами, а также с внешней средой.

Задачей является поиск и использование такого набора свойств и методов агентов как объектов, который позволил бы в наибольшей степени использовать преимущества мультиагентного подхода.

В программном комплексе «Мультиагентная система распространения компьютерных червей в полносвязных гетерогенных сетях «MASWorm»» предлагается формальное описание построенной модели. Агент может быть рассмотрен как набор параметров:

$$a = \langle s, s_t, c, l \rangle, \ a \in A, s \in S, c \in C, \quad (1)$$

где s_t – время пребывания агента в состоянии s; A – количество агентов; S – количество возможных состояний; l – продолжительность жизни; C – множество ячеек рабочей области.

Множество состояний агента определено предварительно и является постоянным. В разработанной модели мы определяем множество состояний как:

$$S=\{Susceptible, Antidotal, Infected, Detected, Recovered\}. \quad (2)$$

где Susceptible – агент здоров. Это состояние агентов, которые восприимчивы к заражению определенным червем, Antidotal – агент здоров. Агенты в этом состоянии имеют установленное антивирусное программное обеспечение, поэтому не могут быть заражены, Infected – агент инфицирован и может быть переносчиком вируса на другие хосты, Detected – заражение агента выявлено антивирусным программным обеспечением и изолировано из сети, Recovered – агент излечен и более не восприимчив к данному типу червя.

Анализ разработанной мультиагентной модели показал, что существуют два фактора, влияющие на распространение сетевого червя Code Red: динамические меры противодействия, предпринятые Интернет-провайдером и пользователями, и замедление скорости распространения сетевого червя, поскольку стремительное размножение червя Code Red вызвало замедления и проблемы с некоторыми маршрутизаторами. Учитывая динамические аспекты человеческих контрмер и переменную скорость инфицирования, нами получена более точная модель распространения сетевого червя, в сравнении с детерминированными аналитическими моделями. Результаты моделирования, а также численное решение показывают, что построенная мультиагентная модель в высокой степени совпадает с наблюдаемыми реальными данными червя Code Red. В частности, это объясняет снижение попыток сканирования хостов в течение нескольких последних часов распространения червя, ни одна из предыдущих детерминированных моделей не способна объяснить данное явление.