Опубликовано: Климентьев К.Е. Моделирование распространения и взаимодействия самовоспроизводящихся объектов // В сб. «Известия Самарского научного центра РАН» №16(2). – Самара: Изд-во СНЦ РАН, 2014. – С. 313-317.

МОДЕЛИРОВАНИЕ РАСПРОСТРАНЕНИЯ И ВЗАИМОДЕЙСТВИЯ САМОВОСПРОИЗВОДЯЩИХСЯ ОБЪЕКТОВ

К.Е. Климентьев, СГАУ

1.Общая характеристика проблемы. Под самовоспроизводящимися объектами в данной работе понимаются сущности окружающего мира, определяющим свойством которых является способность к созданию собственных копий. Этим свойством обладают, например, живые организмы, возбудители эпидемических заболеваний в природе, компьютерные вирусы и черви, информационные сообщения в социальных сетях и т.п.

Исследование динамики их поведения сводится к решению довольно обширного класса задач, частично охарактеризованного, например, в /1/. Некоторые из этих задач восходят к хорошо исследованным моделям «эпидемического распространения», «гибели и размножения», «межвидовой конкуренции», «хищник-жертва» и пр. Однако особый интерес в последние десятилетия представляет подмножество задач, дополнительным условием которых является целенаправленное поведение объектов. Интерес к задачам такого рода появился в связи с проблемой эпидемий вредоносных компьютерных программ и феноменом распространения информации в социальных сетях. Решение этих задач позволяет производить:

- исследование поведения популяции объектов в заданных условиях;
- параметрическую идентификацию модели их поведения, т.е. оценивание условий распространения по зарегистрированным характеристикам поведения;
- выявление факторов, влияющих на динамику распространения;
- изучение возможности управления динамикой путем изменения действующих факторов и внесения новых.

Традиционные методы решения подобных задач основываются на мониторинге реальных процессов, протекающих в природе, обществе, компьютерных и социальных сетях. Недостатками традиционных методов являются высокая стоимость процедуры мониторинга, неполнота собранных сведений, невоспроизводимость результатов, затрудненность (а порой, и невозможность) экспериментального влияния на процессы и т.п. Выйти за пределы этих естественных ограничений позволяет моделирование процессов.

При дальнейшем рассмотрении сконцентрируем внимание на моделировании распространения вредоносных программ: сетевых червей в локальных сетях и сети Интернет, почтовых червей среди абонентов E-mail, компьютерных вирусов с компьютера на компьютер и мобильных червей с одного смартфона на другой. В соответствии с терминологией работы /8/ самокопирующиеся объекты, способные к размножению и перемещению с

одного компьютера на другой, назовем «мобильными агентами».

2.Натурное моделирование. В данном случае моделирование заключается в построении ограниченных сегментов реальных сетей, в которых распространяются реальные мобильные агенты или их имитаторы. Силами преподавателей и студентов факультета информатики СГАУ реализована среда для натурного моделирования распространения мобильных агентов в компьютерных сетях /3/. В отличие от аналога, описанного в /7/, она:

- легко масштабируема, позволяет сужать и расширять масштабы сети;
- использует не реальные вредоносные программы, а их программные «имитаторы»;
- легко конфигурируема, позволяет варьировать параметрами эксперимента (топологией сети, средней скоростью размножения и удаления, алгоритмом поиска адресов для перемещения и пр.).

Рис. 1 – Моделирование размножения мобильного агента в локальной сети: количество узлов N=35, коэффициент размножения β=0.2 ед/сек, поиск адресов – случайный.

Важным достоинством подобных моделей является легкость соблюдения технических особенностей моделируемых систем: пропускной способности сетей, различного быстродействия компьютеров, особенностей различных версий операционных систем и т.п. Так же, при увеличении масштабов сети автоматически воспроизводятся эффекты, характерные для реальных сетей, например, уменьшение их пропускной способности. Однако, с увеличением масштабов модели существенно возрастает стоимость эксперимента.

Целесообразно использовать натурное моделирование для получения исходных числовых характеристик компонентов модели, которые в дальнейшем могут быть использованы для построения моделей других типов. Так же, натурные модели могут использоваться в качестве «эталонов» для исследования адекватности моделей других типов.

3.Аналитическое моделирование. Модели размножения мобильных агентов описываются системами дифференциальных уравнений вида:

$$\left\{\begin{array}{l}\partial I/\partial T = F(I,S,R)\\ \partial S/\partial T = G(I,S,R)\\ \partial R/\partial T = H(I,S,R)\end{array}\right\}, \qquad (1)$$

где T – время; I – множество инфицированных, S – множество здоровых, R – множество «вылеченных» узлов; F, G и H – некоторые функции. Наиболее простые модели на «гомогенных» графах (например, с уравнениями Мальтуса и Фергюльста) решаются аналитически, однако уже модели типа Кермака-МакКендрика - только численно.

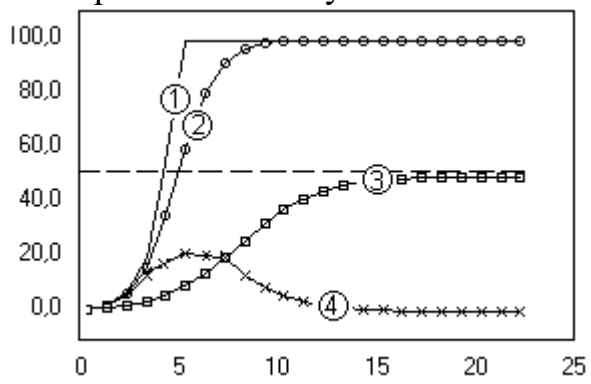
Таблица 1 – Наиболее простые законы поведения и взаимодействия

SI-модель простого экспоненциаль-ного размножения	$\frac{\partial I(t)}{\partial t} = \beta I(t)$
SI-модель размножения в условиях ограниченности ресурсов (например, при случайном характере поиска целей для заражения)	$\frac{\partial I(t)}{\partial t} = \beta I(t) - \beta I^2(t)/N$
SIS-модель размножения в условиях простой конкуренции (например, при удалении вируса с компьютера и возможности повторного заражения)	$\frac{\partial I(t)}{\partial t} = \beta I(t) - \beta I^2(t)/N - \gamma I(t)$
SIR-модель размножения (например, при удалении вируса с компьютера и запрете повторного заражения)	$\left\{ \begin{array}{l} \frac{\partial I(t)}{\partial t} = \beta I(t)\left(\frac{N - I(t) - R(t)}{N}\right) - \gamma I(t) \\ \frac{\partial R(t)}{\partial t} = \gamma I(t) \end{array} \right\}$
Модель подавления «контрагентом», активно сканирующим адресное пространство, удаляющим «агента» и «вакцинирующим» узел	$\left\{ \begin{array}{l} \frac{\partial R(t)}{\partial t} = R(t)\gamma\left(\frac{N - R(t)}{N}\right); \\ \frac{\partial I(t)}{\partial t} = I(t)\beta\left(\frac{N - I(t) - R(t)}{N}\right) - R(t)\gamma\frac{I(t)}{N} \end{array} \right\}$
Модель подавления «контрагентом», использущим принцип «контратаки», а затем удаляющим «агента» и «вакцинирующим» узел	$\left\{ \begin{array}{l} \frac{\partial R(t)}{\partial t} = \gamma I(t)\frac{R(t)}{N} \\ \frac{\partial I(t)}{\partial t} = \gamma I(t)\left(\frac{N - R(t) - I(t)}{N}\right) - \gamma I(t)\frac{R(t)}{N} \end{array} \right\}$

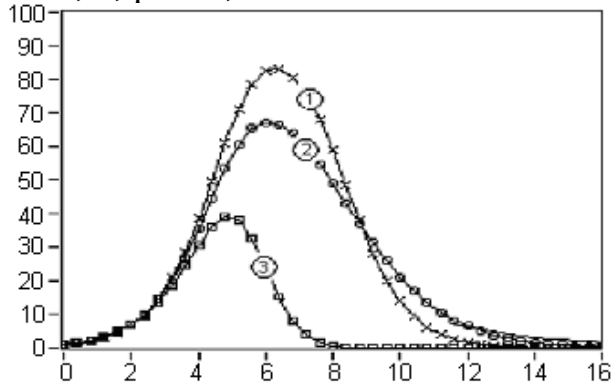
Модель подавления «контрагентом», сочетающем активное сканирование и «контратаку»	$\left\{ \begin{array}{l} \dfrac{\partial R(t)}{\partial t} = \gamma R(t)\left(\dfrac{N - R(t)}{N}\right) + \beta I(t)\dfrac{R(t)}{N}; \\ \dfrac{\partial I(t)}{\partial t} = \beta I(t)\left(\dfrac{N - R(t) - I(t)}{N}\right) - \beta I(t)\dfrac{R(t)}{N} - \gamma R(t)\dfrac{I(t)}{N} \end{array} \right\}$

Чаще всего объектом изучения на аналитических моделях является асимптотическое поведение мобильных агентов – т.е. на интервале времени, стремящемся к бесконечности, и в сетях с однородной структурой. При этом игнорируются, например, неоднородность сети, непостоянство условий во времени и т.п. Так же, важным недостатком подобных моделей является их непрерывный характер, в то время, как реальное поведение мобильных агентов дискретно как во времени, так и по уровню. Это приводит к существенным нарушениям адекватности подобных моделей, особенно в случаях с малым масштабом сети /6/ - подтверждение см. на рис. 1.

Тем не менее, аналитический подход позволяет исследовать наиболее простые, но часто встречающиеся законы распространения и взаимодействия мобильных агентов (см. табл. 1). В этой таблице и далее: β - «коэффициент размножения», γ - «коэффициент подавления», N - количество узлов сети. Дифференциальные уравнения для SI-, SIS- и SIR-моделей хорошо известны /1,6,9/, рис. 2,а. Системы уравнений для размножения в условиях подавления «контрагентом» получены самостоятельно /2,5/, рис. 2,б.



а) Модели размножения: 1 – простое экспоненциальное, 2 – SI, 3 – SIS, 4 – SIR.



б) Модели подавления: 1 – активный «контрагент», 2 – контратакующий, 3 – их комбинация

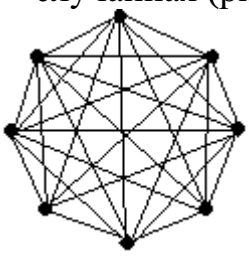
Рис. 2 - Численные решения дифференциальных уравнений для N=100, β=2, γ=1.

Аналитическое моделирование позволяет, например, выбрать правильный закон размножения и противодействия для «контрагента». Так, в 2003 г. «контрчервь» Welchia, противодействующий червю Lovesan, использовал принцип активного сканирования сети и в результате вызвал собственную эпидемию. В то же время, даже по рис. 2,б можно сделать вывод, что червь, использующий контратакующую стратегию (кривая 2), был бы почти так же эффективен, как и сканирующий (кривая 1), но не вызвал бы негативных последствий.

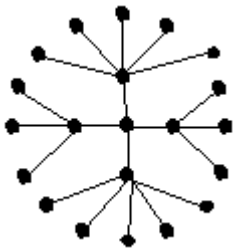
4.Имитационное моделирование. Наиболее общие методы исследования эпидемий мобильных агентов основаны на имитационных моделях. Такой

подход позволяет избавиться от недостатков, присущих аналитическим моделям, учесть большинство факторов и исследовать степень их влияния на развитие эпидемий. Вот некоторые из этих факторов /3,6,9/:

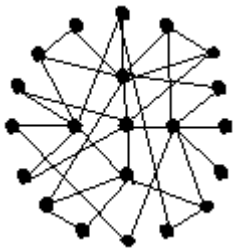
- по мере развития эпидемии возрастает сетевой трафик, снижается пропускная способность линий связи и падает значение коэффициента β;
- эффективные антивирусные средства разрабатываются и начинают работу с задержкой в несколько часов или суток, соответственно, на разных этапах развития эпидемии применимы разные модели;
- имеется прирост числа N за счет машин, вновь подключаемых к сети, с другой стороны, так же наблюдается уменьшение N за счет отключения перегруженных хостов и серверов;
- величина N изменяется в зависимости от времени суток по синусоиде - днем возрастает, ночью падает;
- определенная часть машин содержит «врожденный» иммунитет (например, за счет использования незнакомых вирусу версий операционной системы);
- зато другая часть уязвимых машин по разными причинам просто никогда не вакцинируется вообще и, будучи зараженной, продолжает продолжительное время «фонить»;
- возможен различный характер поиска мобильными агентами целей для поражения – случайный, последовательное сканирование, контратакующий, «морской бой» (учитывается то обстоятельство, что активные IP-адреса в Интернете встречаются группами) и т.п.;
- большое влияние на динамику распространения агентов оказывает топология связей узлов атакующей сети – гомогенная («каждый с каждым» - рис. 3, а), безмасштабная (для которой $P_k = N_k / N$ его узлов со степенью k примерно равна $P_k \approx k^{-\gamma}$, где $2 \le \gamma \le 3$ - рис. 3,б), случайная (рис. 3,в) и т.п.



а) Гомогенная – модель адресного пространства Интернета



б) Безмасштабная – модель структуры связей абонентов E-mail



в) Случайная – модель взаимодействия смартфонов по Blutooth

Рис 3. Варианты сетевых топологий

Большинство исследований распространения самовоспроизводящихся объектов выполняется именно с использованием методов имитационного моделирования. Например, параметрическая идентификация моделей размножения червя Codered II в 2001 г. позволила оценить коэффициент размножения $1.5<\beta<2$ ед/с и начальное условие $I_0=1$ /9/. Однако, методы

имитационного моделирования требуют повышенного внимания к соблюдению требований по адекватности результатов моделирования и, как следствие, наличия как априорной, так и апостериорной информации о параметрах реальных сетей и характеристиках реальных эпидемий. Эти данные могут быть получены в результате мониторинга как реальных процессов, так и процессов, протекающих в натурных моделях.

Силами преподавателей и студентов факультета информатики СГАУ ведется работа над реализацией системы для имитационного моделирования распространения мобильных агентов в компьютерных сетях. Она должна моделировать влияние всех перечисленных выше факторов, включая различные топологии сетей (в том числе, «реалистичные» /4/), непостоянство коэффициентов размножения и подавления, большое количество противоборствующих процессов и пр.

Литература

1. Братусь А.С., Новожилов А.С., Платонов А.П. Динамические системы и модели биологии. - М.: Физматлит, 2010. – 400 с.

2. Климентьев К.Е. Компьютерные вирусы и антивирусы: взгляд программиста. – М.: ДМК-Пресс, 2013. – 656 с.

3. Климентьев К.Е., Помянский Р.В. Три подхода к моделированию сетевых эпидемий // В сб. «ПИТ-12». - Самара: Самар. гос. Аэрокосм. ун-т, 2012. – С. 31-34.

4. Климентьев К.Е. Применение ГИС-технологий при исследовании распространения вредоносных программ // В сб. «Геоинформационные технологии в проектировании и создании корпоративных информационных систем». – Уфа: изд-во УГАТУ, 2012. – С. 123-126.

5. Климентьев К.Е. Аналитические модели взаимодействия мобильных агентов // В сб. «ПИТ-2013». – Самара: Самар. гос. Аэрокосм. ун-т., 2013 – С. 54-56.

6. Leveille J. Epidemic spreading in Technological Networks. – Bristol: HP Laboratories, 2003. – 100 pp.

7. Монахов Ю.М., Мигачева И.А. Экспериментальное исследование распространения вредоносной программы по компьютерной сети // В сб.: Комплексная защита объектов информатизации: Комитет по информатизации, связи и телекоммуникациям Администрации Владимирской области, 2008.

8. Shoch J.F., Hupp J.A. The «Worm» Programs – Early Experience with a Distributed Computation // CACM, 25(3):172-180, March, 1982.

9. Weaver N.C. Warhol Worms: The potential for very fast internet plagues? - 2001. - Режим доступа: http://www1.icsi.berkeley.edu/nweaver/papers/warhol/warhol.html.