МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ЗАЩИТЫ КОМПЬЮТЕРНОЙ СЕТИ С ПОМОЩЬЮ ДИНАМИЧЕСКОГО КАРАНТИНА

MATHEMATICAL MODELING OF COMPUTER NETWORK SECURITY SYSTEM USING DYNAMIC QUARANTINE

N. Semykina

Annotation

In the article the mathematical model of worm propagation under dynamic quarantine is considered. The model is described as the discrete problem of optimal control. The necessary conditions of optimality are formulated. Numerical simulations are provided for Slammer worm epidemic.

Keywords: computer virus, mathematical model, dynamic quarantine, discrete task, optimal control.

Семыкина Наталья Александровна
К.ф–м.н., доцент,
ФГБОУ ВПО "Тверской Государственный университет"

Аннотация

Рассматривается математическая модель распространения вирусов в компьютерной сети с учетом динамического карантина. Данная модель формализуется как дискретная задача оптимального управления. Сформулированы необходимые условия оптимальности. Получено численное решение для примера эпидемии сетевого червя SQL Slammer.

Ключевые слова:

Компьютерный вирус, математическая модель, динамический карантин, дискретная задача, оптимальное управление.

С каждым годом растет количество атак вредоносного программного обеспечения на инфраструктуру вычислительных сетей всех уровней. По статистическим данным только за последние пять лет поток вирусов в сети Интернет увеличился в шесть раз [1]. Вирусные атаки приобретают форму глобальный сетевых эпидемий, благодаря сети Интернет и большим пропускным способностям каналов передачи информации. Поэтому исследования в области защиты компьютерных сетей необходимы и актуальны. Одним из способов исследования является математическое моделирование.

Авторы статьи [2] рассмотрели и обосновали применение одного из средств автоматического смягчения распространения эпидемии сетевого червя – динамический карантин. Под динамическим карантином подразумевается техническое устройство, которое срабатывает каждый раз, когда компьютер ведет себя атипично, блокируя трафик. Через определенный промежуток времени хост с карантина выпускают, даже если он не был проверен на наличие вируса. Построенная модель в [2] не лишена недостатков.

Во–первых, авторы предполагали, что лечение компьютеров будут производить сотрудники службы безопасности (т.е. в ручном режиме). Однако, скорость лечения инфицированных хостов рассматривалась как постоянная функция на всем промежутке времени исследования, не зависящая от времени. А это больше соответствует автоматическому режиму.

Во–вторых, авторы не учли иммунизацию неинфицированных компьютеров. В реальных же условиях лечение и иммунизация происходит одновременно за счет установки антивирусного программного обеспечения или установки специально разработанного патча. При этом иммунитет приобретают не только инфицированные компьютеры, но и уязвимые.

Построим математическую модель, учтя эти недостатки. Используем предложенный в [2] вид функции роста числа зараженных компьютеров для описания динамики численности компьютеров. Данную модель формализуем как дискретную задачу. Введем следующие обозначения: S^i – число неинфицированные хостов, восприимчивых к заражению вирусом в i–й период времени, при этом

$$i = \overline{0,q}$$

I^i – количество зараженных машин в в i–й период времени

$$i = \overline{0,q}$$

R^i – число хостов невосприимчивых к вредоносному коду,

т. е. невосприимчивых хостов в i–й период времени.

Тогда, в любой момент времени будет выполняться условие $S^i + I^i + R^i = N^i$, где $i = \overline{0,q}$

Величины u^i и v^i, $i = \overline{0,q-1}$

будем рассматривать как управления, которые характеризуют иммунизацию и лечение восприимчивых и инфицированных компьютеров в i–й период времени.

На управление накладывается ограничения, связанные с техническими и экономическими возможностями

$$u^i \ge 0, \quad v^i \ge 0, \quad 0 \le u^i + v^i \le U_{\max}, \; i = \overline{0,q-1} . \quad (1)$$

Динамика численности узлов компьютерной сети всех типов описывается рекуррентными соотношениями: ,

$$\begin{aligned} S^{i+1} &= S^i + \tau\left(bS^i - \beta^i S^i I^i - \mu S^i - u^i S^i\right) \\ I^{i+1} &= I^i + \tau\left(\beta^i S^i I^i - v^i I^i - \mu I^i\right) \\ R^{i+1} &= R^i + \tau\left(u^i S^i + v^i I^i - \mu R^i\right) \end{aligned} \quad (2)$$

где $S^0 = S_0$, $I^0 = I_0$, $R^0 = R_0$, – фиксировано,

$$\beta^i = \tilde{\beta}\frac{1 + v^i T_k}{1 + (\lambda_1 + v^i)T_k} \cdot \frac{1}{1 + \lambda_2 T_k}, \quad i = \overline{0,q}$$

Здесь

τ – временной параметр,

b – параметр, характеризующий скорость прироста новых уязвимых узлов,

μ – коэффициент, характеризующий постоянную скорость отключения компьютеров от сети, при этом отключение не связано с вирусной атакой.

$\tilde{\beta}$ – скорость распространения вируса,

$1/\lambda_1$ – время, за которое инфицированный узел будет обнаружен и помещен на карантин,

$1/\lambda_2$ – время, в течение которого подозрительный узел не являющимся зараженным помещается на карантин, Tk – общее время карантина.

Целью противовирусных мероприятий для компьютерной сети будет условие, чтобы в конечный момент времени q большая часть компьютеров (не менее 80%) являлись невосприимчивыми к заражению, т.е.

$$R^q \ge 0{,}8N^q, \quad \text{где } N^q = S^q + I^q + R^q.$$

Учтем данное ограничение в функционале с помощью положительной срезки. Тогда дискретная задача оптимального управления будет состоять в минимизации функционала

$$J([u,v]) = A\left[\max\{0; 0{,}8N^q - R^q\}\right]^2, \quad (3)$$

где $A > 0$ – масштабирующий множитель.

В силу выпуклости множества достижимости в данной задаче справедливо необходимое условие оптимальности в виде принципа максимума для дискретных задач оптимального управления.

Теорема.

Пусть система управления описывается уравнениями (2) и

$$u^i, v^i, \; i = \overline{0,q-1}, \; S^i, \; I^i, \; R^i, \; i = \overline{0,q},$$

соответственно оптимальные управления и оптимальные траектории, минимизирующие функционал (3). Все функции задачи (1) – (3) являются непрерывно дифференцируемыми. Тогда если множества допустимости выпуклы, найдутся такие не все равные нулю векторы

$$p_S^{i+1}, \quad p_I^{i+1}, \quad p_R^{i+1}, \quad i = \overline{1,q},$$

что выполняются условия:

1)
$$\begin{aligned} &p_S^i - p_S^{i+1}\left(1 - \tau(\beta^i I^i + \mu + u^i)\right) - \\ &- p_I^{i+1}\tau\beta^i I^i - p_R^{i+1}\tau u^i = 0, \quad i = \overline{1,q-1}, \\ &p_I^i - p_I^{i+1}\left(1 + \tau(\beta^i S^i - \mu - v^i)\right) + \\ &+ p_S^{i+1}\tau\beta^i S^i - p_R^{i+1}\tau v^i = 0, \quad i = \overline{1,q-1}, \\ &p_R^i - p_R^{i+1}(1 - \tau\mu) = 0, \quad i = \overline{1,q-1}. \end{aligned}$$

2)
$$\begin{aligned} p_S^q &= p_I^q = -1{,}6A\left[\max\{0; 0{,}8N^q - R^q\}\right] \\ p_R^q &= 0{,}4A\left[\max\{0; 0{,}8N^q - R^q\}\right] \end{aligned}$$

3) *оптимальное управление определяется из решения задачи максимизации нелинейного программирования*

$$\begin{aligned} &\sum_{i=0}^{q-1}\tau\left(\tilde{\beta}\frac{1 + v^i T_k}{1 + (\lambda_1 + v^i)T_k} \cdot \frac{1}{1 + \lambda_2 T_k} S^i I^i (p_I^{i+1} - p_S^{i+1}) + \right. \\ &\left. + u^i S^i (p_R^{i+1} - p_S^{i+1}) + v^i I^i (p_R^{i+1} - p_I^{i+1})\right) \to \max_{u,v} \\ &u^i \ge 0, \quad v^i \ge 0, \quad 0 \le u^i + v^i \le U_{\max}, \quad i = \overline{1,q} . \end{aligned}$$

Исследуем задачу (1) – (3) на конкретном примере. Для этого рассмотрим одну из эпидемий сетевого червя SQL Slammer [3, 4].

Данный вирус в январе 2003 года за 10 минут атаковал и инфицировал около 75 тыс. компьютеров по всему миру. На ранней стадии число зараженных машин удваивалось каждые 8,5 секунды. Через три минуты после запуска вирус сканировал уже 55 млн. хостов в секунду.

В результате этого было поражено около 500000 серверов, и отключило Южную Корею от интернета на 12

часов.

В Соединенных Штатах произошли перебои в работе оборудования, подключенного к сети Internet, так например, возникли проблемы с системой резервирования авиабилетов, происходили задержки рейсов, а также перестали работать 13 тысяч банковских автоматов [3, 4].

Для построения численного решения воспользуемся методом градиентного спуска.

Используем следующие параметры:

$\tilde{\beta} = 0{,}0698$,
$\lambda_1 = 0{,}2$,
$\lambda_2 = 0{,}00002315$,
$b = 0{,}00001$,
$\mu = 0{,}00001$,
$Tk = 0{,}016$.

Результаты численных экспериментов представлены в виде графиков функций.

Ниже на **рис. 1** представлены результаты сравнения статистических данных исходной модели с учетом карантина и лечения [2] и модифицированной модели (1) – (3).

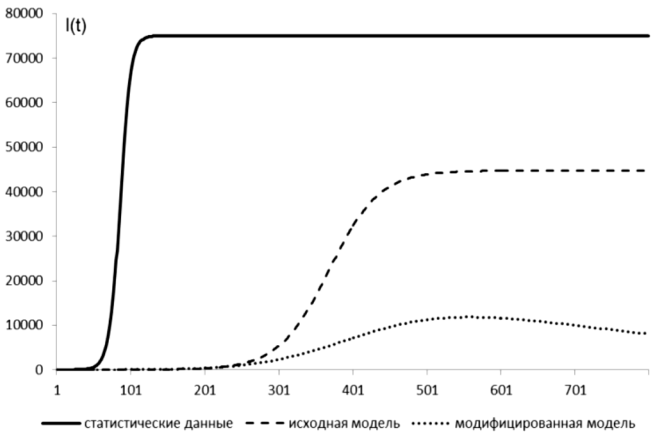

Рисунок 1. Динамика распространения сетевого червя *Slammer*.

Как можно заметить из представленных графиков учет лечения зараженных и иммунизации неинфицированных хостов в виде функции управления, зависящей от времени, дает наилучший результат. То есть, фактор сдерживания в виде динамического карантина может существенно замедлить распространение вредоносного кода. А если на начальном этапе установить специально разработанный патч, то это может помочь предотвратить развитие эпидемии компьютерных вирусов.

ЛИТЕРАТУРА

1. https://www.av-test.org/en/statistics/malware/ (дата обращения 10. 08. 2015)
2. C. C. Zou, W. Gong, and D. Towsley. Worm Propagation Modeling and Analysis under Dynamic Quarantine Defense. ACM CCS Workshop on Rapid Malcode (WORM'03), Oct. 27, Washington DC, USA, 2003.
3. Последний компьютерный вирус побил рекорды скорости распространения инфекции [Электронный ресурс]. – Режим доступа: http://www.newsru.com/world/04feb2003/slammer.html (дата обращения 9. 08. 2015)
4. D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, N. Weaver. Inside the Slammer Worm // IEEE Security and Privacy, vol. 1, № 4, pp. 33–39, Aug 2003. URL: http://www.icir.org/vern/papers/IEEESP03.pdf (дата обращения 9. 08. 2015)