Математические структуры и моделирование
2006, вып. 16, с. 84–87

УДК 681.3

НАХОЖДЕНИЕ ВРЕМЕНИ ЗАРАЖЕНИЯ ЛОКАЛЬНОЙ СЕТИ ВИРУСАМИ НА ОСНОВЕ СЕТИ ФОРМАЛЬНЫХ НЕЙРОНОВ

С.В. Белим, С.Ю. Белим

Рассмотрена модель локальной вычислительной сети как сети формальных нейронов со ступенчатой функцией отклика. Проведено моделирование распространения вредоносных программ в локальной сети. Показана зависимость времени распространения вирусов от топологии сети.

Возможность моделирования распространения «вирусных» программ в локальной вычислительной сети вытекает из того, что каждая рабочая станция может находиться только в двух состояниях – «зараженном» и «незараженном». В качестве возможных процессов взаимодействия рабочих станций будем рассматривать обмен информацией. В данной работе рассматривается только случай одноранговой сети, поэтому средняя интенсивность обмена информацией между любой парой рабочих станций считается одной и той же. Также необходимо предусмотреть защиту от вирусов, которая может быть двух видов. Во-первых, это межсетевые экраны, препятствующие проникновению вредоносных программ, а во-вторых, антивирусные программы, обнаруживающие «вирусы» и уничтожающие их.

Построим формальную модель вычислительной сети, отражающую процесс распространения «вирусных» программ. Прежде всего сопоставим локальной сети невзвешенный граф, вершины которого представляют собой отдельные рабочие станции. Случай невзвешенного графа соответствует одноранговой сети, для рассмотрения сети с выделенным сервером необходимо ребрам графа сопоставить веса, соответствующие относительной интенсивности информационного обмена между двумя рабочими станциями.

Зараженность i-ой рабочей станции в момент времени t будем описывать величиной $S_i(t)$, которая может принимать два значения:

$$S_i(t) = \begin{cases} 1, & \text{если «заражен»;} \\ 0, & \text{иначе.} \end{cases} \qquad (1)$$

Каждую рабочую станцию будем представлять как формальный нейрон. При этом роль синапсов будут играть ребра графов, а величина $S_i(t)$ – характеристика

Омский государственный университет.
E-mail: belim@univer.omsk.su

аксона. Как и в других моделях, время в компьютерной сети можно рассматривать как дискретную величину, тогда состояние отдельного нейрона в момент времени t будет определяться сигналами, поступившими в предыдущий момент времени $t-1$. Сигнал, передаваемый по синапсам, может иметь два значения – 0 или 1. Ноль соответствует информации, не содержащей вредоносных программ, а единица – распространению «вируса». Будем считать вирусы активными, то есть «зараженная» рабочая станция передает только «зараженную» информацию.

Наличие межсетевых экранов у рабочих станций будет выражаться величиной r_i, определяющей пороговое значение объема вредоносной информации, выше которого происходит переключение нейрона в единичное значение, что соответствует заражению рабочей станции. Однако это пороговое значение может повышаться или понижаться в результате деятельности пользователя. Причем деятельность пользователя носит случайный характер как по времени воздействия на систему защиты, так и по величине. В результате выполнения задач, решаемых на рабочей станции, уровень защиты может как повышаться, так и понижаться. Кроме того, пользователь может инициировать процессы, которые могут «вылечивать» зараженный компьютер. Этот процесс также носит случайный характер. Чтобы учесть описанные случайные процессы, в модель необходимо ввести случайную величину, воздействующую на уровень защищенности. В дальнейшем межсетевой экран в момент времени t будет записываться в виде $r_i(1-\zeta(i,t))$, где $\zeta(i,t)$ – случайная величина с нормальным распределением.

Важную роль в нейронных сетях играет функция отклика отдельного нейрона $\theta(v)$, где v – сигнал, подаваемый на синапсы. В данной работе был рассмотрен простейший случай ступенчатой функции отклика:

$$\theta(v) = \begin{cases} 1, & \text{если } v \geq 0; \\ 0, & \text{если } v < 0. \end{cases} \tag{2}$$

Таким образом, состояние рабочей станции в i-ом узле в момент времени t может быть найдено из соотношения:

$$\begin{aligned} ot_i &= S_i + \sum S_j(t-1) - r_i(1-\zeta(i,t_{n-1})), \\ S_i(t) &= \theta(ot_i - r_i(1-\zeta(i,t-1))) = \begin{cases} 1, & \text{если } ot \geq r_i(1-\zeta(i,t-1)); \\ 0, & \text{если } ot < r_i(1-\zeta(i,t-1)). \end{cases} \end{aligned} \tag{3}$$

Здесь ot_i – суммарное воздействие «вирусов» соседних узлов на i-ую рабочую станцию, суммирование производится по ближайшим соседям (индекс j пробегает номера узлов, непосредственно связанных с i-ым). Рабочая станция переходит в зараженное состояние, если воздействие вирусов превышает порог защиты.

Введем вектор состояния системы в момент времени $V(t)$ в момент времени t в пространстве $\{0,1\}^N$, где N – количество узлов сети. Координатами $V(t)$ будут величины $S_i(t)$:

$$V(t) = (S_1(t), S_2(t), ..., S_N(t)). \tag{4}$$

Обозначим через M матрицу связности графа сети, тогда эволюция системы во времени будет описываться уравнением:

$$V(t) = \Theta(V(t-1) + M \cdot V(t-1) - R \cdot (I - Z(t))). \tag{5}$$

Здесь Θ - ступенчатая вектор-функция, $R = (r_1, r_2, ..., r_N)$ – вектор пороговых значений уровня защиты рабочих станций, I – единичная матрица, $Z(t)$ – матрица случайных величин.

$$Z(t) = \begin{pmatrix} \zeta_1(t) & 0 & ... & 0 \\ 0 & \zeta_2(t) & ... & 0 \\ ... & ... & ... & ... \\ 0 & 0 & ... & \zeta_N(t) \end{pmatrix}. \tag{6}$$

Для характеристики скорости заражения введем время перехода локальной сети в зараженное состояние T как минимальное время, через которое все рабочие станции оказываются «зараженными» ($S_i(T) = 1$,$i = \overline{1, N}$).

Очевидно, что наибольшим временем заражения обладает линейная цепочка с начальным заражением крайней рабочей станции, так как в каждый момент времени может быть заражена только одна рабочая станция, и каждый узел испытывает воздействие только одного соседнего узла. Обозначим время заражения линейной цепочки через T_0. Для сетей, обладающих другой топологией, введем относительное время заражения:

$$\tau = \frac{T}{T_0}. \tag{7}$$

В начальный момент времени заражена только одна рабочая станция $S_1(0) = 1$, $S_2(0) = 0$, ..., $S_N(0) = 0$.

Авторами были рассмотрены различные топологии локальных вычислительных сетей, для которых уравнение (1) решалось численно. Для каждой топологии локальной сети время заражения вычислялось 10 раз с дальнейшим усреднением. Так, для широко распространенных топологий «кольцо» и «звезда» были получены значения $T_r = 0.5$ и $T_s = 2/N$ при $r_i = 0.5$ для всех $i = \overline{1, N}$.

Далее был осуществлен поиск схем соединения $N = 20$ рабочих станций, обладающих наибольшим относительным временем заражения τ для одинакового порогового значения $r = 0.5$ для всех рабочих станций.

Поиск наиболее устойчивых к заражению топологий сети осуществлялся методом Монте-Карло. В качестве исходной бралась матрица связности, состоящая только из единиц. Затем применялся следующий алгоритм:

1. Изменяем выбранный случайным образом элемент матрицы.
2. Вычисляем время заражения.
3. Если, в результате такого изменения, время заражения увеличивается, то новая топология считается более выгодной и оставляется, иначе происходит возврат к прежней матрице связности.
4. Переход к пункту 1.

Алгоритм выполняется до тех пор, пока изменения в матрице связности не приводят к увеличению времени заражения. При реальных расчетах вычисления

прерывались, если пятьдесят подряд следующих попыток изменения матрицы отбрасывались.

Вычисления показали, что наличие петель и ответвлений в линейной цепочке существенно уменьшает время заражения.

References

1. Нейроинформатика / А.Н.Горбань, В.Л.Дунин-Барковский, А.Н.Кирдин и др. Новосибирск: Наука. Сибирское предприятие РАН, 1998.
2. Уоссермен Ф. Нейрокомпьютерная техника. М.: Мир, 1992.