УДК 519.872: 004.2

О ПРИМЕНЕНИИ G-СЕТЕЙ ПРИ МОДЕЛИРОВАНИИ ПОВЕДЕНИЯ ВИРУСОВ И КОМПЬЮТЕРНЫХ АТАК И ПРОГНОЗИРОВАНИИ РАСХОДОВ ОТ НИХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ И СЕТЯХ

В.В. Науменко, М.А. Маталыцкий

В работе представлены методы и методики исследования в переходном режиме сетей массового обслуживания с отрицательными заявками и некоторыми особенностями, в том числе с доходами, применяемых при нахождении вероятностно-временных характеристик и доходов в информационных системах и сетях с учетом попадания в них вирусов или DDoS-атах на них.

Введение

При проектировании реальных объектов часто необходимо уметь моделировать их текущее поведение, находить различные характеристики, зависящие от времени. Обработка запросов в информационных системах и сетях (ИСС) может осуществляться по различным правилам. В таких случаях важной задачей является нахождение вероятностей состояний их моделей – марковских и произвольных сетей массового обслуживания (СеМО) с различными особенностями в переходном (нестационарном) режиме.

В данной работе рассматривается класс СеМО, который может применяться при моделировании поведения вирусов и компьютерных атак в ИСС в нестационарном режиме. А именно – сетей с положительными и отрицательными заявками (G-сетей массового обслуживания [1]), в которых заявки перед обслуживанием могут подвергаться нестандартным перемещениям (уничтожаться, не получив обслуживания).

Для многих ИСС часто приходится решать задачи, связанные с оценкой их производительности с учетом стоимости. Кроме того, при исследовании ИСС важной задачей является оценка стоимостных доходов, которые они получают от функционирования их различных подсистем, например, серверов.

При попадании вируса в ИСС из-за потери информации или ее искажения ИСС несет некоторые расходы или убытки. Для учета расходов и их прогнозирования в таких ИСС предложено использовать G-сети с доходами и некоторыми особенностями (сигналами\триггерами, сигналами со случайной задержкой). Доходами от переходов в ИСС могут являться онлайн-платежи, денежные переводы и т. п. пользователей систем интернет-банкинга и других схожих систем. Положительными заявками при этом являются запросы интернет-пользователей, а отрицательными заявками могут быть вирусы в таких ИСС или массовые запросы в случае DDoS-атаки на ИСС. Такие сети могут использоваться при прогнозировании доходов и потерь при использовании Web-серверов Nginx.

G-сети с различными особенностями и их вероятностно-временные характеристики

Пусть в систему массового обслуживания (СМО) S_i извне поступает поток положительных (обычных) заявок с интенсивностью λ_{0i}^{+} и пуассоновский поток отрицательных заявок с интенсивностью λ_{0i}^{-}, $i=\overline{1,n}$. Все поступающие в сеть потоки заявок являются независимыми. Отрицательная заявка, поступающая в некоторую систему сети, в которой имеется одна положительная заявка, мгновенно уничтожает одну из них. После этого она сама сразу же выходит из сети, не получив в этой СМО обслуживания. В каждой СМО сети могут обслуживаться только положительные заявки. Каждая положительная заявка направляется в СМО S_i с вероятностью p_{0i}^{+}, а отрицательная – с вероятностью p_{0i}^{-}, $\sum_{i=1}^{n} p_{0i}^{+} = \sum_{i=1}^{n} p_{0i}^{-} = 1$, $i=\overline{1,n}$. Положительная заявка, которая получила обслуживание в СМО S_i, с вероятностью p_{ij}^{+} направляется в *j*-ую СМО как положительная заявка, а с вероятностью p_{ij}^{-} – как отрицательная заявка и с вероятностью $p_{i0} = 1 - \sum_{j=1}^{n}\left(p_{ij}^{+} + p_{ij}^{-}\right)$ уходит из сети во внешнюю среду, $i, j = \overline{1,n}$.

Состояние СеМО записывается в виде вектора $k(t) = (k,t) = (k_1, k_2, \ldots, k_n, t)$, где $k_i(t)$ – число заявок в *i*-ой СМО сети, $i=\overline{1,n}$.

Основными задачами являются: нахождение нестационарных распределений вероятностей состояний $P(k,t)$, средних характеристик и ожидаемых доходов с целью их оптимизации.

Определим *n*-мерную производящую функцию

$$\Psi_n(z,t) = \sum_{k_1=0}^{\infty}\sum_{k_2=0}^{\infty}\ldots\sum_{k_n=0}^{\infty} P(k,t)\prod_{i=1}^{n} z_i^{k_i},\ z=(z_1,z_2,\ldots,z_n),\ |z|<1. \qquad (1)$$

В работах [2; 3] выведена система разностно-дифференциальных уравнений (РДУ), которой удовлетворяют вероятности состояний такой сети. Доказано утверждение о выражении для производящей функции (1). Полагается, что такая СеМО функционирует в режиме высокой нагрузки. Как указано в монографии [4], ИСС довольно часто функционируют на определенных интервалах времени в режиме такой нагрузки. Показано, что производящую функцию можно представить в виде многократного сходящегося степенного ряда:

$$\Psi_n(z,t) = a_0(t)\sum_{l_1=0}^{\infty}\ldots\sum_{l_n=0}^{\infty}\ \sum_{q_1=0}^{\infty}\ldots\sum_{q_n=0}^{\infty}\ \sum_{r_1=0}^{\infty}\ldots\sum_{r_n=0}^{\infty}\ \sum_{u_1=0}^{\infty}\ldots\sum_{u_n=0}^{\infty} t^{\sum_{i=1}^{n}(l_i+q_i+r_i+u_i)} \times$$

$$\times\prod_{i=1}^{n}\left[\frac{\left(\lambda_{0i}^{+}\right)^{l_n}\left(\mu_i p_{i0}+\lambda_{0i}^{-}\right)^{q_i}\mu_i^{r_i+u_i}\left(\prod_{j=1}^{n}p_{ij}^{+}\right)^{r_i}\left(\prod_{j=1}^{n}p_{ij}^{-}\right)^{u_i}}{l_i!\,q_i!\,r_i!\,u_i!}z_i^{\alpha_i+l_i-q_i-r_i+R-u_i-U}\right],$$

где $a_0(t)=\exp\left\{-\sum_{i=1}^{n}\left(\lambda_{0i}^{+}+\lambda_{0i}^{-}+\mu_i\right)t\right\}$.

Получены аналогичные результаты для открытой G-сети с положительными заявками и сигналами. Учет в моделях ИСС сигналов позволяет управлять нагрузкой в них. В СМО S_i извне поступает дополнительный поток сигналов, который является пуассоновским с интенсивностью λ_{0i}^{-}, $i=\overline{1,n}$. Поступающий сигнал мгновенно перемещает положительную заявку из *i*-ой СМО в *j*-ую СМО с вероятностью q_{ij}, в этом случае сигнал называют триггером; с вероятностью $p_{i0}=1-\sum_{j=1}^{n}q_{ij}$ сигнал может сработать как отрицательная заявка и уничтожить в СМО S_i положительную заявку. В работе [5] выведена система РДУ, которой удовлетворяют вероятности состояний такой сети. Доказано утверждение о выражении для производящей функции (1), с помощью которого получено соотношение для среднего числа заявок.

В [6] проведен анализ G-сети со случайной задержкой сигналов. Вероятность того, что положительная заявка обслужится в СМО S_i за время $[t,t+\Delta t)$, если в данной СМО в момент времени t имеется k заявок, равна $\mu_i^{+}(k)\Delta t+o(\Delta t)$. Положительная заявка, которая получила обслуживание в СМО S_i с вероятностью p_{ij}^{+} направляется в СМО S_j снова как положительная заявка, а с вероятностью p_{ij}^{-} – как сигнал. Каждый поступающий сигнал активизируется в течение некоторого случайного интервала времени. Вероятность того, что поступивший в СМО S_i сигнал активизируется за время $[t,t+\Delta t)$, при условии, что в этой СМО в момент времени t имеется l неактивизированных сигналов, равна $\mu_i^{-}(l)\Delta t+o(\Delta t)$. По истечении времени активизации: либо с вероятностью q_{ij}^{+} сигнал срабатывает как триггер, и перемещает положительную заявку из СМО S_i в СМО S_j, при этом данная заявка остается положительной; либо с вероятностью q_{ij}^{-} сигнал снова срабатывает как триггер, переместив одну положительную заявку из СМО S_i в СМО S_j, но при этом данная заявка в СМО S_j становится сигналом; либо с вероятностью $q_{i0}=1-\sum_{j=1}^{n}\left(q_{ij}^{+}+q_{ij}^{-}\right)$ сигнал срабатывает как отрицательная заявка, которая, уничтожает положительную заявку в СМО S_i и покидает сеть.

Под состоянием сети в момент времени t будем понимать вектор $k(t)=(k,l,t)=((k_1,l_1,t),(k_2,l_2,t),...,(k_n,l_n,t))$, который образует однородный марковский процесс со счетным числом состояний, где состояние (k_i,l_i,t) означает, что в момент времени t в СМО S_i находятся k_i положительных заявок и l_i неактивизированных сигналов, $i=\overline{1,n}$. В [6] получена система РДУ, которой удовлетворяют вероятности состояний такой G-сети.

Определим $2n$-мерную производящую функцию

$$\Psi_{2n}(z,t)=\sum_{k_1=0}^{\infty}...\sum_{k_n=0}^{\infty}\sum_{l_1=0}^{\infty}...\sum_{l_n=0}^{\infty}P(k,l,t)\prod_{i=1}^{n}z_i^{k_i}z_{n+i}^{l_i},\ |z|<1. \qquad (2)$$

Предполагается, что $k_i(t)>0$ и $l_i(t)>0$ $\forall t>0$, $i=\overline{1,n}$. Доказана теорема о выражении для производящей функции (2), с помощью которого получены соотношения для среднего числа положительных заявок и неактивизированных сигналов. В качестве применения полученных результатов описана модель компьютерной атаки и эффект проникновения вируса в компьютерную сеть.

Прогнозирование расходов в информационных сетях с помощью G-сетей с доходами

В работе [7] рассматривается G-сеть с учетом ее доходов и расходов при обслуживании положительных и отрицательных заявок. Вначале исследуется случай, когда доходы от переходов между состояниями сети являются детерминированными функциями, зависящими от состояний сети и времени. Получена система РДУ для ожидаемых доходов систем сети. Для каждой СМО она может быть представлена в общем виде

$$\frac{dV(k,t)}{dt}=-\Lambda(k)V(k,t)+\sum_{i,j=0}^{n}\left[\Phi_{ij1}(k)V(k+I_i-I_j,t)-\Phi_{ij2}(k)V(k-I_i-I_j,t)\right]+A(k), \qquad (3)$$

где $V(k,t)$ – ожидаемый доход, который получает некоторая система сети за время t, если в начальный момент времени сеть находилась в состоянии k, $\Lambda(k)$, $\Phi_{ij1}(k)$, $\Phi_{ij2}(k)$ – некоторые ограниченные неотрицательные функции. В случае, когда доходы от переходов между состояниями сети не зависят от времени, для решения системы (3) с бесконечным числом дифференциальных уравнений предложено использовать алгоритм, основанный на применении модифицированного метода последовательных приближений, совмещенного с методом рядов. Это позволяет находить ожидаемые доходы систем сети за приемлемое процессорное время.

Пусть $v_m(k,t)$ – приближение ожидаемого дохода $v(k,t)$ на m-й итерации, $v_{m+1}(k,t)$ – решение системы (3), с помощью метода последовательных приближений:

$$v_{m+1}(k,t)=+\frac{\mathrm{A}(k)}{\Lambda(k)}\left[1-e^{-\Lambda(k)t}\right]+e^{-\Lambda(k)t}\left\{V(k,0)+\right.$$

$$\left.+\int_0^t e^{\Lambda(k)x}\sum_{i,j=0}^{n}\left[\Phi_{ij1}(k)v_m(k+I_i-I_j,x)-\Phi_{ij2}(k)v_m(k-I_i-I_j,x)\right]dx\right\},\ m=0,1,2,... \qquad (4)$$

Очевидно, что $v_m(k,0)=v(k,0)$, и пусть также $v_0(k,t)=v(k)=\lim_{t\to\infty}v(k,t)$.

Доказано, что последовательные приближения $v_m(k,t)$, $m=1,2,\ldots$, сходятся при $t\to\infty$ к стационарному решению системы уравнений (3), если оно существует. Указаны случаи, когда такое решение существует и когда нет. Для практического применения рассматриваемого метода более важны следующие утверждения.

Теорема 1.. *Последовательность* $\{v_m(k,t)\}$, $m=0,1,2,\ldots$, *построенная с помощью соотношения (4), при любом ограниченном по* t *нулевом приближении* $v_0(k,t)$ *сходится при* $m\to\infty$ *к единственному решению системы РДУ (3).*

Теорема 2. *Любое приближение* $v_m(k,t)$, $m\ge 1$, *представимо в виде сходящегося степенного ряда* $v_m(k,t)=\sum_{l=0}^{\infty} d_{ml}(k)t^l$, *коэффициенты которого удовлетворяют рекуррентным соотношениям:*

$$d_{m+1l}(k)=\frac{\left[-\Lambda(k)\right]^l}{l!}\left\{V(k,0)-\frac{\mathrm{A}(k)}{\Lambda(k)}+\sum_{u=0}^{l-1}\frac{(-1)^{u+1}D_{mu}(k)}{\left[\Lambda(k)\right]^{u+1}}u!\right\},\ l\ge 0,$$

$$d_{m+10}(k)=v(k,0),\quad d_{0l}(k)=v(k,0)\delta_{l0},$$

где $D_{ml}(k)=\sum_{i,j=0}^{n}\left[\Phi_{ij1}(k)d_{ml}\left(k+I_i-I_j\right)-\Phi_{ij2}(k)d_{ml}\left(k-I_i-I_j\right)\right]$, δ_{l0} *– символ Кронекера. Если* $\Lambda(k)\ge 1$, *то ряд для* $v_m(k,t)$ *сходится при любом конечном* $t>0$.

В [8] рассмотрена еще одна методика, основанная на применении многомерных z-преобразований. Введя в рассмотрение многомерные z-преобразования для ожидаемых доходов систем сети

$$\varphi_i(z,t)=\sum_{k_1=0}^{\infty}\sum_{k_2=0}^{\infty}\ldots\sum_{k_n=0}^{\infty}v_i(k_1,k_2,\ldots,k_n,t)z_1^{k_1}z_2^{k_2}\cdot\ldots\cdot z_n^{k_n}=\sum_{\substack{k_i=\overline{0,}\\ i=\overline{1,n}}}^{\infty}v_i(k,t)\prod_{l=1}^{n}z_l^{k_l},\ |z|<1,\ i=\overline{1,n},$$

получены для них соотношения, на основе которых предложен алгоритм нахождения ожидаемых доходов в открытой G-сети.

Рассматривается также случай, когда доходы от переходов между состояниями G-сети являются случайными величинами с заданными моментами первых двух порядков [9]. Используя методику для нахождения ожидаемых доходов, основанную на использовании найденных приближенных и точных выражений для средних значений случайных доходов, получено выражение для ожидаемых доходов

$$v_i(t)=v_{i0}+\left[\lambda_{0i}^{+}a_{0i}-\lambda_{0i}^{-}\overline{a}_{0i}-\mu_i\left(b_{i0}p_{i0}+\sum_{j=1}^{n}\left(a_{ij}p_{ij}^{+}+c_{ij}p_{ij}^{-}\right)\right)+\sum_{j=1}^{n}\mu_j a_{ji}p_{ji}^{+}+d_i\right]t,\ i=\overline{1,n},$$

где a_{0i}, $\overline{a}_{0i}$, b_{i0}, a_{ij}, a_{ji}, c_{ij}, d_i – соответствующие математические ожидания.

В [10] исследована G-сеть с доходами и сигналами со случайной задержкой, когда доходы от переходов между состояниями сети являются СВ, а параметры сети зависят от времени. Получено также выражение для ожидаемых доходов и найдены дисперсии доходов.

В [11] проведен анализ G-сети с многолинейными системами, вероятностями переходов заявок между ними, зависящими от времени, и

случайными доходами от переходов между ее состояниями. Получено выражение для ожидаемых доходов. Рассмотрены частные случаи практического применения такой сети для случая сетевой DDoS-атаки ИСС. Сформулирована и решена оптимизационная задача, связанная с максимизацией доходов G-сети в переходном режиме по числу линий обслуживания заявок в многолинейных СМО.

Заключение

В данной работе приведены выражения для многомерных производящих функций вероятностей состояний G-сетей, включая сети с сигналами и сети со случайной задержкой сигналов в случае, когда они функционируют в условиях высокой нагрузки. С помощью этих выражений можно находить вероятности состояний и среднее число заявок в системах в виде многократных рядов в переходном режиме.

Представлены методы нахождения ожидаемых доходов в системах G-сетей с доходами с вышеуказанными особенностями в случаях, когда доходы от переходов между их состояниями являются детерминированными функциями, зависящими от состояний сети и времени или случайными величинами с заданными моментами первого и второго порядков. В первом случае они основаны на получении систем РДУ для ожидаемых доходов и использовании предложенных способов решения этих систем. Во втором случае найдены приближенные соотношения для ожидаемых доходов систем. С помощью полученных результатов были решены задачи максимизации ожидаемых доходов в G-сетях по числу линий обслуживания в системах.

Разработанные методы позволяют повысить эффективность и качество проектирования различных ИСС и других объектов, моделями которых являются вышеуказанные СеМО. В частности, полученные результаты, позволяют моделировать поведение вирусов в ИСС, проводить прогноз расходов ИСС при DDoS-атаках, и управлять нагрузкой в ИСС.

Список литературы

1. Gelenbe, E. Product form queueing networks with negative and positive customers / E. Gelenbe // Journal of Applied Probability. – 1991. – Vol. 28. – P. 656–663.
2. Науменко, В.В. Анализ сети с положительными и отрицательными заявками в переходном режиме / В.В. Науменко, М.А. Маталыцкий // Вестник ГрГУ. Сер. 2. Математика, физика, информатика, вычислительная техника и управление. – 2013. – № 3 (159). – С. 135–142.
3. Matalytski, M. Non-stationary analysis of queueing network with positive and negative messages / M. Matalytski, V. Naumenko // Journal of Applied Mathematics and Computational Mechanics. – 2013. – Vol. 12, № 2. – P. 61–71.
4. Вишневский, В.М. Теоретические основы проектирования компьютерных сетей / В.М. Вишневский. – М. : Техносфера, 2003. – 506 с.

5. Matalytski, M. Investigation of G-network with signals at transient behavior / M. Matalytski, V. Naumenko // Journal of Applied Mathematics and Computational Mechanics. – 2014. – Vol. 13, Is. 1. – P. 75–86.
6. Маталыцкий, М.А. Анализ G-сети со случайной задержкой сигналов в переходном режиме и ее применение / М.А. Маталыцкий, В.В. Науменко // Вестник ГрГУ. Сер. 2. Математика, физика, информатика, вычислительная техника и управление. – 2014. – № 1 (170). – С. 135–147.
7. Науменко, В.В. Анализ доходов в марковских G-сетях методом последовательных приближений / В.В. Науменко // Вестник ГрГУ. Сер. 2. Математика, физика, информатика, вычислительная техника и управление. – 2014. – № 1 (170). – С. 125–134.
8. Matalytski, M. Application of a z-transforms method for investigation of Markov G-networks / M. Matalytski, V. Naumenko // Journal of Applied Mathematics and Computational Mechanics. – 2014. – Vol. 13, Is. 1. – P. 61–73.
9. Науменко, В.В. Анализ марковских сетей с доходами, положительными и отрицательными заявками / В.В. Науменко, М.А. Маталыцкий // Информатика. – 2014. – № 1 (41). – С. 5–14.
10. Науменко, В.В. Исследование и применение G-сети с доходами и сигналами со случайным временем активизации / В.В. Науменко, М.А. Маталыцкий // Вестник ГрГУ. Сер. 2. Математика, физика, информатика, вычислительная техника и управление. – 2014. – № 3 (180). – С. 142–152.
11. Науменко, В.В. Анализ и оптимизация G-сети с многолинейными системами и доходами / В.В. Науменко // Информационные процессы. – 2014. – Т. 14, № 4. – С. 295–306.

Науменко Виктор Викторович, старший преподаватель кафедры стохастического анализа и эконометрического моделирования факультета математики и информатики Гродненского государственного университета имени Янки Купалы, кандидат физико-математических наук, victornn86@gmail.com

Маталыцкий Михаил Алексеевич, заведующий кафедрой стохастического анализа и эконометрического моделирования факультета математики и информатики Гродненского государственного университета имени Янки Купалы, доктор физико-математических наук, профессор, m.matalytski@gmail.com