ИЗВЕСТИЯ РАН. ТЕОРИЯ И СИСТЕМЫ УПРАВЛЕНИЯ, 2020, № 5, с. 106–115

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ

УДК 519.85

АНАЛИЗ КРИТИЧЕСКИ ОПАСНЫХ ПОВРЕЖДЕНИЙ СЕТИ СВЯЗИ. I. МОДЕЛЬ И ВЫЧИСЛИТЕЛЬНЫЙ ЭКСПЕРИМЕНТ

© 2020 г. Ю. Е. Малашенко[a,]*, И. А. Назарова[a]
[a]ФИЦ ИУ РАН, Москва, Россия
*e-mail: irina-nazar@yandex.ru

Поступила в редакцию 20.03.2020 г.
После доработки 09.04.2020 г.
Принята к публикации 25.05.2020 г.

В рамках вычислительных экспериментов на потоковой модели сети связи и управления изучаются изменения системных функциональных характеристик при разрушающих воздействиях. В качестве критически опасного повреждения рассматривается подмножество ребер, при удалении которых хотя бы для одной пары узлов источник-приемник отсутствуют любые пути соединения. Для каждого повреждения определяется как общее число разъединенных пар-корреспондентов, так и все направления связи, пропускная способность которых оказывается меньше заданного нормативного значения. На основе полученных данных формируются многопараметрические диаграммы оценки изменения максимально возможных потоков для каждого разделяющего разреза и всех пар вершин. Граничные точки на диаграммах соответствуют наиболее опасным повреждениям, недоминируемым хотя бы по одному показателю ущерба. Анализируются результаты последствий разрушающих воздействий на сетевые системы с различными структурными особенностями.

DOI: 10.31857/S0002338820050108

Введение. В работе излагаются результаты вычислительных экспериментов на модели многопользовательской сети связи и управления. Анализируются изменения значений предельно-допустимых потоков между всеми парами узлов при разрушении ребер. Рассматриваются критически опасные повреждения, при которых хотя бы для одной пары источник-приемник отсутствует возможность установить связь.

Оценка последствий конкретного разрушения производится по двум критериям: число разъединенных пар источник-приемник и/или уменьшение пропускной способности каналов связи между всеми корреспондентами. Величина ущерба для каждой пары вычисляется как разность максимальных значений потока в исходной и поврежденной сети [1]. Расчеты по указанным критериям позволяют получить представительные векторные оценки, с помощью которых можно выделить наиболее опасные разрушающие воздействия.

Вычислительные эксперименты проводились для сетей с различными структурными особенностями. Для всех сетей сформированы соответствующие многопараметрические диаграммы, позволяющие сравнивать критически опасные повреждения с недоминируемыми векторными оценками ущерба.

Предложенный метод можно рассматривать как один из подходов к решению классической задачи исследования операций “оборона против нападения” [2–5]. Полученные диаграммы позволяют “обороняющейся стороне” в условиях неопределенности сравнивать возможные потери при разрушении ребер минимальных и вершинных разрезов.

Вершинные разрезы изучаются при поиске критически важных элементов (узлов) сети в [6–8], с использованием различных векторных критериев – в [9, 10]. При анализе уязвимости кластерных конгломератов обычно проводится агрегированная оценка потерь суммарного предельно-допустимого потока из центрального узла ко всем остальным [11, 12].

В последние годы возрос интерес к более предметному и комплексному анализу уязвимости сложных взаимосвязанных сетевых систем различного назначения, функционирующих как единое территориально-распределенное образование [13–15]. В [14] прослеживается эволюция моделей исследования уязвимости, отмечается необходимость специального анализа влияния человеческого фактора, а также террористических действий и/или спланированных хакерских атак. В [16] рассматривается влияние природных катастроф на региональные сети связи, в [17, 18] предлагаются технические решения по управлению сетевым трафиком в условиях чрезвычайных ситуаций, охватывающих большие территории. В [19] приводится одна из возможных классификаций различных повреждающих воздействий на сетевые информационные системы. В [20–23] основное внимание уделяется изучению уязвимости сетевых распределенных систем топливно-энергетического комплекса. Далее в данной работе предлагается вычислительная схема, использующая методы многокритериального анализа и потокового программирования, которая может быть применена при анализе уязвимости сетевых систем различного назначения [24, 25].

1. Математическая модель. Для анализа последствий повреждений многопользовательской сетевой системы связи и управления используется модель передачи многопродуктового (МП) потока. Граф сети $G(d)$ без петель и сдвоенных ребер задается множествами $\langle V, R\rangle$: узлов (вершин графа) сети $V = \{v_1, v_2, \ldots, v_n, \ldots, v_N\}$; неориентированных ребер $R = \{r_1, r_2, \ldots, r_k, \ldots, r_E\} \subset V \times V$.

Пусть ребро r_k соединяет узлы с номерами n_k, j_k, $r_k = (v_{n_k}, v_{j_k}) = (n_k, j_k)$. Для описания направления передачи потоков по сети каждому ребру r_k, $k = \overline{1, E}$, ставятся в соответствие две ориентированные дуги u_k, u_{k+E}, прямого и обратного направления из множества направленных дуг $U = \{u_1, u_2, \ldots, u_k, \ldots, u_{2E}\}$ графа сети $G(d)$, $r_k \Leftrightarrow \{u_k, u_{k+E}\}$. Обозначим через $K(v_n)$ множество номеров ребер $r_k \in R$, инцидентных вершине v_n:

$$K(v_n) = \{k \,|\, r_k \in R\};$$

$S(v_n)$ – множество номеров исходящих дуг, по которым поток покидает узел v_n; $T(v_n)$ – множество номеров входящих дуг, по которым поток поступает в узел v_n.

Множества $S(v_n)$, $T(v_n)$ однозначно определяются следующей процедурой. Пусть некоторое ребро $r_k \in R$ соединяет вершины с номерами n и j, такими, что $n < j$. Тогда ориентированная дуга $u_k = (v_n, v_j)$ считается *исходящей* из вершины v_n и ее номер k заносится в множество $S(v_n)$, а ориентированная дуга $u_{k+E} = (v_j, v_n)$ – *входящей* для v_n и ее номер $k + E$ помещается в список $T(v_n)$. Соответственно дуга u_k является *входящей* для v_j и ее номер k попадает в $T(v_j)$, а дуга u_{k+E} – *исходящей* и номер $k + E$ заносится в список $S(v_j)$ исходящих дуг.

В рамках модели предполагается, что между любой парой узлов передаются различные потоки, например, происходят телефонные разговоры или двигаются пассажиропотоки между станциями метро. Пара узлов-корреспондентов p_m определяется упорядоченной парой вершин $p_m = (v_{s_m}, v_{t_m})$, где вершина с номером s_m называется источником, а с номером t_m – стоком или приемником потока m-го вида. В настоящей работе в сети из N узлов рассматривалось $M = N(N-1)$ независимых, невзаимозаменяемых и равноправных потоков различных видов, которые передаются между узлами-корреспондентами из множества $P = \{p_1, p_2, \ldots, p_M\} \subset V \times V$. Величины указанных потоков считаются функциональными характеристиками сети. В ходе вычислительных экспериментов изучаются изменения предельно-возможных потоков для каждой пары p_m при разрушении ребер сети.

Пусть x_{mk} – величина потока m-го вида, который передается в МП-сети по ребру r_k, $x_{mk} \geq 0$, $m = \overline{1, M}$, $k = \overline{1, E}$. Каждому ребру $r_k \in R$ приписывается число d_k, определяющее предельно-допустимый поток, который можно пропустить через r_k в обоих направлениях. В исходной сети компоненты вектора пропускных способностей – $d = (d_1, d_2, \ldots, d_k, \ldots, d_E)$ – наперед заданные положительные числа $d_k > 0$. Вектором d определяются следующие ограничения на потоки, передаваемые по ребру r_k:

$$\sum_{m=1}^{M} (x_{mk} + x_{m(k+E)}) \leq d_k, \quad x_{mk} \geq 0, \quad x_{m(k+E)} \geq 0, \quad k = \overline{1, E}. \tag{1.1}$$

Обозначим через z_m, $z_m \geq 0$, величину потока m-го вида, который поступает в сеть в узле с номером s_m и покидает ее из узла с номером t_m.

Во всех узлах $v_n \in V$, $n = \overline{1,N}$, сети для всех видов потоков должны выполняться условия сохранения потоков:

$$\sum_{i \in S(v_n)} x_{mi} - \sum_{i \in T(v_n)} x_{mi} = \begin{cases} z_m, & \text{если } v_n = v_{s_m}, \\ -z_m, & \text{если } v_n = v_{t_m}, \\ 0 & \text{в остальных случаях,} \end{cases} \tag{1.2}$$
$$n = \overline{1,N}, \quad m = \overline{1,M}, \quad x_{mi} \geq 0, \quad z_m \geq 0.$$

Величина z_m равна входящему потоку m-го вида, который пропускается от источника к стоку пары p_m при распределении потоков x_{mi} по дугам сети.

Ограничения (1.1), (1.2) задают множество достижимых векторов потоков $z = (z_1, z_2, \ldots, z_m, \ldots, z_M)$:

$$Z(x,d) = \{z \geq 0 \,|\, (z,x) \text{ удовлетворяют } (1.1), (1.2)\} \tag{1.3}$$

при передаче в МП-сети для всех пар $p_m \in P$.

В настоящей работе анализируются результаты вычислительных экспериментов и изучаются оценки изменения максимальных величин потоков для всех возможных пар узлов $M = N(N-1)$ при структурных повреждениях ребер сети.

2. Формирование множества структурных повреждений. Рассмотрим некоторую произвольную пару узлов-корреспондентов $p_m \in P$ и определим максимально возможный поток, который можно передать в сети $G(d)$ из вершины с номером s_m в вершину с номером t_m без учета всех остальных потоков.

З а д а ч а 1. При некотором фиксированном m найти максимальный поток из узла с номером s_m в узел с номером t_m:

$$z_m^0 = \max_{z,x}\{z_m \,|\, z \in Z(x,d)\}.$$

Согласно [1], каждому максимальному значению z_m^0 соответствует некоторый набор ребер – минимальный разрез R_m, $R_m \subset R$. Множество номеров ребер, образующих разрез R_m, обозначим

$$h(m) = \left\{ k \,|\, r_k \in R_m, z_m^0 = \sum_{k \in h(m)} d_k \right\},$$

где R_m – минимальное подмножество ребер, таких, что при удалении их из сети максимальный поток из v_{s_m} в v_{t_m} становится равным нулю, а вершины с номерами s_m и t_m оказываются в разных связных компонентах графа сети $G(d)$. Последовательно для всех $p_m \in P$, $m = \overline{1,M}$, решаются цепочки задач 1 и формируется вектор максимальных потоков

$$z^0 = (z_1^0, z_2^0, \ldots, z_m^0, \ldots, z_M^0).$$

Вектору z^0 ставится в соответствие множество

$$H(\cdot) = \{h(1), h(2), h(3), \ldots, h(m), \ldots, h(M)\}$$

номеров ребер, найденных при решении последовательности задач 1 для всех $p_m \in P$.

Для дальнейшего формирования множества повреждений рассматривается следующая модифицированная сеть. В графе сети $G(d)$ пропускная способность всех ребер полагается равной единице:

$$d_k = 1, \quad k = \overline{1,E},$$

полученный граф сети обозначается $G(1)$, а соответствующее множество достижимых потоков – $Z(x, 1)$:

$$Z(x,1) = \{Z(x,d) \,|\, d_k = 1, k = \overline{1,E}\}.$$

Для $G(1)$ определяется максимальный поток для всех пар $p_m \in P$ как решение следующей задачи максимизации.

З а д а ч а 2. Для некоторой фиксированной пары $p_m \in P$ найти максимальный поток

$$z_m^1 = \max_{z,x}\{z_m \,|\, z \in Z(x,1)\}.$$

Величина z_m^1 равна числу ребер в минимальном разрезе R_m^1 для максимального целочисленного потока из вершины с номером s_m в вершину с номером t_m, $z_m^1 = |R_m^1|$. Обозначим через

$$q(m) = \left\{ k \,|\, r_k \in R_m^1, z_m^1 = \sum_{k \in q(m)} d_k \right\}$$

список номеров ребер, при удалении которых максимальный поток из вершины с номером s_m в вершину с номером t_m становится равным нулю.

По аналогии с множеством $H(\cdot)$ строится множество

$$Q(\cdot) = \{q(1), q(2), \ldots, q(m), \ldots, q(M)\}$$

номеров ребер, входящих в минимальные разрезы, найденные при решении задачи 2 для всех $p_m \in P$, $m = \overline{1, M}$, в сети $G(1)$.

Рассмотрим подмножество

$$y(n) = \{k \,|\, r_k \in R, k \in K(v_n)\}$$

номеров ребер, инцидентных вершине v_n, и сформируем множество

$$Y(\cdot) = \{y(1), y(2), \ldots, y(n), \ldots, y(N)\},$$

состоящее из списков номеров ребер, инцидентных каждой вершине сети.

Для проведения вычислительного эксперимента и анализа возможных повреждений формируется множество уникальных повреждений сети

$$W = \{w_1, w_2, \ldots, w_l, \ldots, w_L\},$$

согласно следующей процедуре. В множествах $H(\cdot)$, $Q(\cdot)$, $Y(\cdot)$ могут содержаться одинаковые элементы. Тождественным спискам номеров ребер $h(\cdot)$, $q(\cdot)$, $y(\cdot)$ ставится в соответствие единственный элемент w_l – список номеров ребер для совпадающих $h(\cdot), q(\cdot)$ или $y(\cdot)$:

$$w_l = \{k \,|\, r_k \in R, k \in h(\cdot), k \in q(\cdot), k \in y(\cdot)\}.$$

3. Оценки повреждений. При проведении вычислительных экспериментов при некотором повреждении w_l пропускная способность ребер сети $G(d(l))$ задается следующим образом:

$$d_k(l) = \begin{cases} d_k, & \text{если} \quad k \notin w_l, \\ 0, & \text{если} \quad k \in w_l. \end{cases}$$

В поврежденной сети $G(d\langle l \rangle)$ для всех $p_m \in P$, последовательно для каждого $m = \overline{1, M}$ определяется возможный максимальный поток.

З а д а ч а 3. При некоторых заданных l и m найти:

$$z_m^0(l) = \max_{z,x}\{z_m \,|\, (x,z) \in Z(x, d(l))\}.$$

Задача 3 решается последовательно для всех p_m, $p_m \in P$, и всех $w_l \in W$. На основе найденных $z_m^0(l)$, $m = \overline{1, M}$, $l = \overline{1, L}$, вычисляются индикаторные показатели:

$$\xi(m,l) = \begin{cases} 1, & \text{если} \quad z_m^0(l) = 0, \\ 0, & \text{если} \quad z_m^0(l) > 0. \end{cases}$$

Для каждого $w_l \in W$ рассчитывается

$$\mu(l) = \frac{\sum_{m=1}^{M} \xi(m,l)}{M}$$

– доля от общего числа пар узлов P, для которых максимальный поток становится равен нулю при данном повреждении w_l.

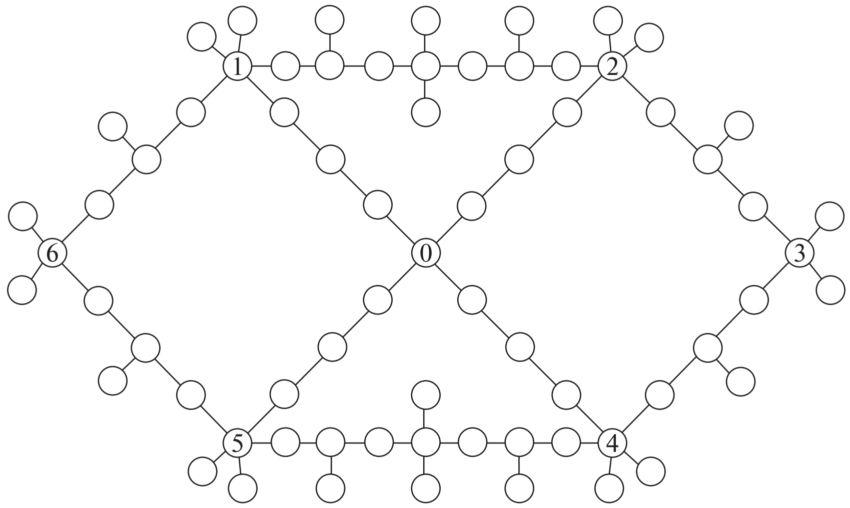

Рис. 1. Базовая сеть

Для всех $m = \overline{1, M}$, $l = \overline{1, L}$, таких, что $z_m^0(l) > 0$, и наперед заданного значения γ вычисляется индикаторная функция

$$\eta(m, l, \gamma) = \begin{cases} 1, & \text{если } \gamma \geq \dfrac{z_m^0(l)}{z_m^0} > 0, \\ 0, & \text{если } \gamma < \dfrac{z_m^0(l)}{z_m^0}. \end{cases}$$

Значения параметра γ задаются априори в диапазоне $0 < \gamma < 1$. Индикатор $\eta(m, l, \gamma) = 1$, если максимальный поток $z_m^0(l)$ для пары p_m при повреждении w_l оказывается не больше критического значения γ.

При заданном γ для некоторого повреждения $w_l \in W$ и $z_m^0(l) > 0$ вычисляется

$$\psi(l, \gamma) = \frac{\sum_{m=1}^{M} \eta(m, l, \gamma)}{M}, \quad l = \overline{1, L},$$

равная доле от общего числа пар узлов P, для которых максимальный поток становится меньше или равен критическому значению при повреждении $w_l \in W$. На основе значений $(\mu(l), \psi(l, \gamma))$ для всех повреждений $w_l \in W$ строятся диаграммы, которые позволяют оценить влияние каждого разрушающего воздействия на потоки между всеми источниками и приемниками. Недоминируемые значения на внешней границе диаграмм дают возможность выделить наиболее "опасные" повреждения, которые разрывают связь между наибольшим числом пар узлов и/или приводят к критически опасному уменьшению потоков ниже допустимых показателей.

4. Вычислительный эксперимент. Вычислительный эксперимент проводился на моделях сетевых систем, представленных на рис. 1, 2 (на рис. 1 – базовая, на рис. 2 слева – рокадная, справа – фронтальная). В каждой из сетей 69 узлов. Пропускные способности ребер выбирались случайным образом из отрезка [900, 999] и совпадают для всех сетей. Пропускная способность каждого из двух дополнительных ребер на рис. 2 равна 900.

Для формирования множества критически опасных повреждений W было найдено порядка 10^4 минимальных разрезов, из которых чуть более 10^2 разрезов вошло в W (около 1%). Для целей анализа и отображения структурных повреждений на диаграммах каждому $w_l \in W$ ставится

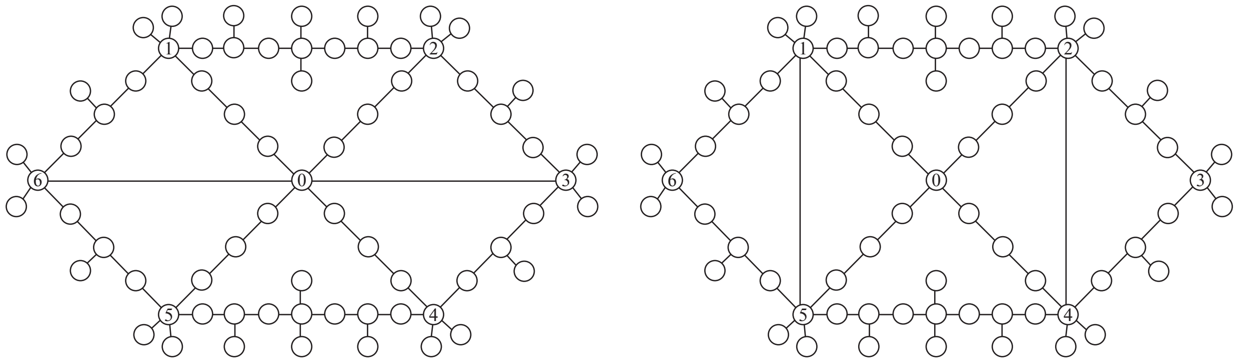

Рис. 2. Рокадная и фронтальная сети

в соответствие “ маска” – тройка индикаторов $str(w_l) = (a, b, c)$, значения которых определяются следующим образом:

$a = 1$, если повреждение w_l совпадает с одним или более списком $h(j)$ в $H(\cdot)$, $a = 0$ – в противном случае;

$b = 1$, если список w_l встречается в множестве $Q(\cdot)$ хотя бы один раз, $b = 0$ – в противном случае;

$c = 1$, если w_l идентичен одному или более элементам в $Y(\cdot)$, $c = 0$ – в противном случае.

Для базовой сети (рис. 1) в множество W было включено всего 125 различных повреждений. В табл. 1 для базовой сети представлены: семь возможных записей строк-индикаторов, соответствующее число повреждений и обозначение последних на диаграммах.

Маска, содержащая только одну единицу, указывает на повреждение, принадлежащее к одному типу разрезов. Таких повреждений в множестве W больше половины и именно эти разрушения приводят к самым большим потерям.

На рис. 3 представлены диаграммы (μ, ψ) для базовой сети при $\gamma = 0.6$ и 0.5. “Жирные точки” у восточного края диаграмм определяют недоминируемые повреждения, разделяющие максимальное число пар-корреспондентов (значение $\mu = 1/48$ по оси абсцисс). Маска (0, 1, 0) соответствует разрезам в сети с графом $G(1)$ при $d_k = 1$, $k = \overline{1, E}$. Согласно табл. 2, существует четыре различных недоминируемых разрушения w_l, приводящих к одинаковому ущербу.

На диаграммах для базовой сети (рис. 3) недоминируемые повреждения с максимальными значениями ψ отмечены “треугольниками”. Указанные разрушения возникают при удалении вершины v_2, а точнее – инцидентных ей ребер. Таким образом удаление вершины приводит к заметному ухудшению качества связи, уменьшению пропускной способности, хотя не сильно влияет на связность графа сети. На диаграммах “треугольники” расположены ближе к оси ординат и имеют бóльшие значения ψ. В табл. 3 приводится максимальное число пар-корреспондентов с различными нарушениями связи для двух недоминируемых разрушений при $\gamma = 0.6$.

Недоминируемые разрушения базовой сети с указанными масками приводят к повреждениям, ущерб от которых различается более чем в 4 раза. Недоминируемый разрез в сети с единичной

Таблица 1

Маска	Число повреждений	Обозначение на диаграмме
100	28	Кольцо
010	23	Жирная точка
001	17	Треугольник
111	35	Крестик
011	17	с указанием числа
110	5	одинаковых
101	0	повреждений

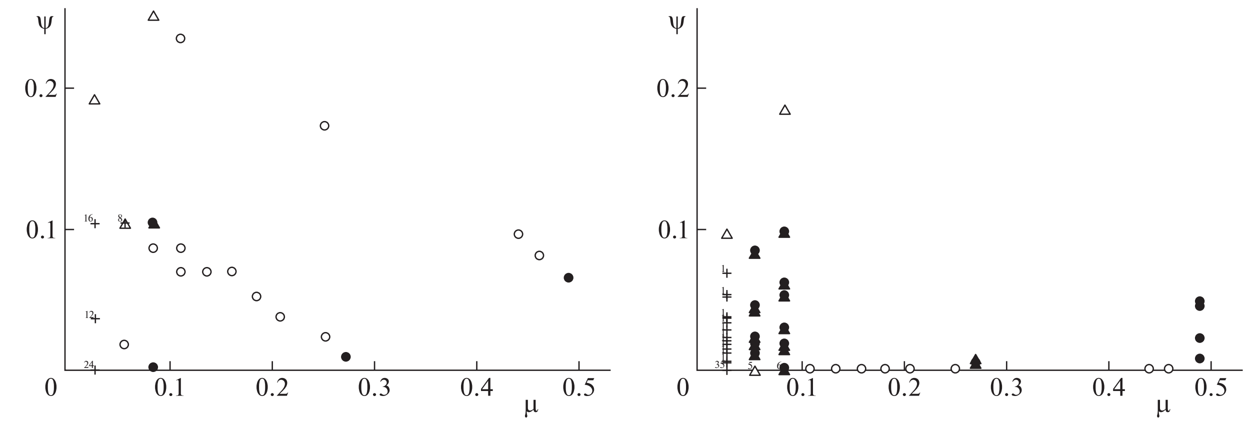

Рис. 3. Диаграммы для базовой сети

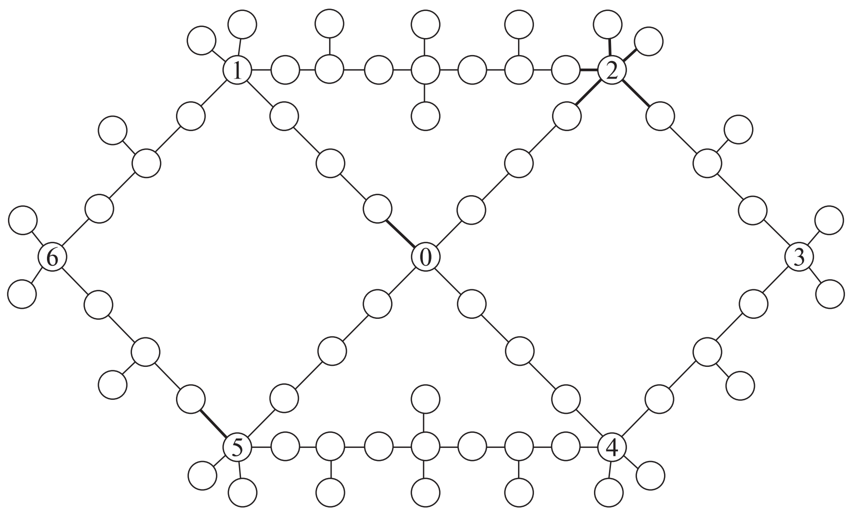

Рис. 4. Наиболее опасные повреждения

пропускной способностью ребер разъединяет половину пар, но только у 7% оставшихся величина потока снижается ниже критического значения $\gamma = 0.6$. Наихудший вершинный разрез – удаление вершины v_2 – разъединяет менее 9% пар, качество связи становится ниже допустимого у 25% пар.

Недоминируемые повреждения для базовой сети при $\gamma = 0.6$ лежат в северо-восточной части диаграммы на рис. 3 слева и обозначены кольцами и жирной точкой. Маска (1, 0, 0) соответствует минимальным разрезам из множества $H(\cdot)$. На рис. 3 справа для базовой сети и $\gamma = 0.5$ повреждения с недоминируемыми значениями ущерба и масками (0, 1, 0), (0, 0, 1) обозначены жирной точкой и остались в северо-восточной части диаграммы, а все кольца переместились в ее внутреннюю часть. Дело в том, что значение $\gamma = 0.5$ задает более жесткие ограничения на величины сохранившихся потоков, но не влияет на число разрывов для линий связи. В результате значения ψ уменьшаются, μ – остается неизменным, а рассматриваемое повреждение перестает быть недоминируемым. На рис. 4 на графе базовой сети отмечены все ребра, входящие хотя бы в одно повреждение из табл. 3.

Таблица 2

Маска	γ	100	010	001	111	011	110	101
Число недоминируемых	$\gamma = 0.6$	4	4	4	–	–	–	–
повреждений	$\gamma = 0.5$	–	1	1	–	–	–	–

Таблица 3

Маска	010	001
Число разъединенных пар	1150	$\gg 200$
Число пар с уменьшением потока ниже $\gamma = 0.6$	150	$\ll 600$

Таблица 4

γ	Сеть	Базовая		Фронтальная		Рокадная	
	Маска	010	001	100	001	010	001
0.6	Число разъединенных пар	1150	200	1080	200	1010	200
	Число пар с уменьшением потока	150	600	200	600	90	480
0.5	Число разъединенных пар	1150	200	1080	200	1010	70
	Число пар с уменьшением потока	110	435	0	435	60	235

Базовая сеть и сети с рис. 2 имеют совпадающие множества узлов и пар-корреспондентов. Диаграммы оценки повреждений для сетей с добавленными ребрами приведены на рис. 5, 6. Добавление двух дополнительных ребер увеличивает число возможных путей соединения и максимальные потоки для большого числа корреспондентов. В табл. 4 помещены число разъединенных пар и число пар, для которых максимально возможные потоки оказываются ниже критического значения γ. Все величины приводятся для двух недоминируемых повреждений, при которых достигается либо максимум числа разъединенных пар (самая восточная точка на диаграммах), либо максимум числа пар, для которых максимальной поток ниже γ (самая северная точка на диаграммах).

Анализ табл. 4 показывает, что базовая сеть более уязвима, поскольку при особо опасных разрушениях большее число корреспондентов (6%) оказываются разъединенными по сравнению с фронтальной и рокадной сетями. Наилучший показатель у рокадной сети – наименьший по ущербу. Полученный результат закономерен, поскольку шесть центральных ребер рокадной сети, инцидентных узлу v_0, затрудняют разделение графа сети на две связанные компоненты. В рокадной сети после повреждений также поддерживается более высокое качество связи – потери потоков меньше. Последнее связано с более мощным транзитным узлом v_0, который усилен двумя дополнительными ребрами. На диаграммах с рис. 5, 6 видно (и анализ табл. 4 это подтверждает), что разрушение минимального разреза из множеств $H(\cdot)$ или $Q(\cdot)$ влечет за собой более серьезные нарушения функционирования сети. Наличие всего двух дополнительных ребер в рокадной сети (по сравнению с базовой) позволяет снизить максимальное число разъединенных пар на 12%, однако не влияет на ухудшение качества связи. Действительно, при разрушении со-

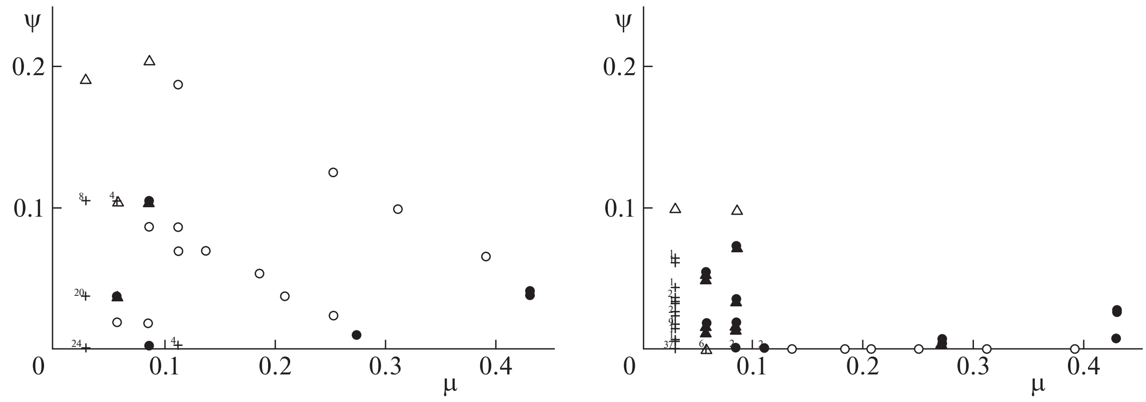

Рис. 5. Диаграммы для рокадной сети

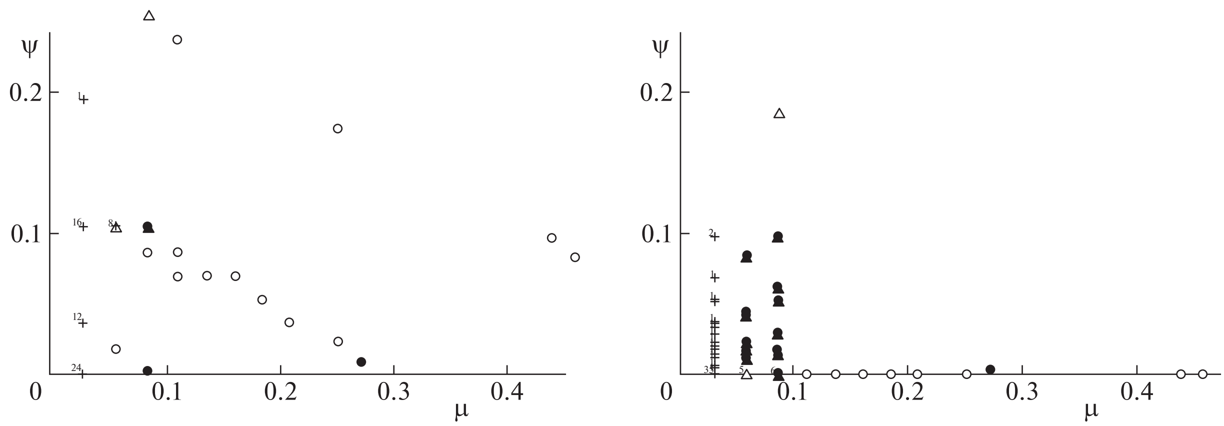

Рис. 6. Диаграммы для фронтальной сети

ответствующих вершинных разрезов падение потоков практически одинаково как в базовой, так и в рокадной сетях (см. табл. 4).

Заключение. При проведении вычислительных экспериментов используются алгоритмы потокового программирования. На первом этапе для каждой пары узлов решается задача поиска максимального потока и минимального разреза. Верхняя оценка числа операций для решения этой задачи составляет $O(N^5)$: всего пар узлов $O(N^2)$, а для определения максимального потока достаточно $O(N^3)$ [26]. На базе полученных минимальных разрезов формируется множество повреждений W, верхняя оценка числа элементов в котором $O(N^2)$. Для каждого повреждения w_l вновь определяются максимальные потоки для всех пар узлов. Результирующая верхняя оценка вычислительных затрат полиномиально зависит от числа узлов в сети и составляет не более $O(N^7)$.

При проведении расчетов для больших сетей можно использовать простые схемы распараллеливания вычислений в гетерогенной вычислительной среде и программные реализации алгоритмов сетевой оптимизации для различных операционных систем. Указанные возможности позволяют производить модельные эксперименты как на кластерах из персональных компьютеров, так и в больших территориально-удаленных центрах.

СПИСОК ЛИТЕРАТУРЫ

1. *Йенсен П., Барнес Д.* Потоковое программирование. М.: Радио и связь, 1984.
2. *Фрэнк Г., Фриш М.* Сети, связь и потоки. М.: Связь, 1978.
3. *Гермейер Ю.Б.* Введение в теорию исследования операций. М.: Наука, 1971.
4. *Dinh T.N., Thai M.T.* Assessing Attack Vulnerability in Networks with Uncertainty // IEEE Conf. on Computer Communications (INFOCOM). Kowloon, 2015. P. 2380–2388.
5. *Малашенко Ю.Е., Назарова И.А., Новикова Н.М.* Один подход к анализу возможных структурных повреждений в многопродуктовых сетевых системах // ЖВМиМФ. 2019. Т. 59. № 9. С. 1626–1638.
6. *Lalou M., Tahraoui M.A., Kheddouci H.* The Critical Node Detection Poblem in Networks: a Survey // Computer Science Review. 2018. V. 28. P. 92–117.
7. *Walteros J., Pardalos P.* Selected Topics in Critical Element Detection // Optimization and its Applications. 2012. V. 71. P. 9–26.
8. *Veremyev A., Prokipyev O.A., Pasiliao E.L.* Critical Nodes for Distance-based Connectivity and Related Problems in Graphs // Networks. 2015. V. 66. Iss. 3. P. 170–195.
9. *Ventresca M., Harrison K.R., Ombuki-Berman B.M.* The Bi-objective Critical Node Detection Problem // European J. Oper. Res. 2018. V. 265. Iss. 3. P. 895–908.
10. *Li J., Pardalos P.M., Xin B., Chen J.* The Bi-objective Critical Node Detection Problem with Minimum Pairwise Connectivity and Cost: Theory and Algorithms // Soft Computing. 2019. V. 23. P. 1–16.
11. *Kuhnle A., Nguyen N.P., Dinh T.N., Thai M.T.* Vulnerability of Clustering under Nodes Failure in Complex Networks // Social Network Analysis and Mining. 2017. V. 7. Iss. 1. P. 8–24.

12. *Малашенко Ю.Е., Назарова И.А., Новикова Н.М.* Анализ кластерных повреждений в сетевых системах // ЖВМиМФ. 2020. Т. 60. № 2. С. 173–184.
13. *Grubesic T.H., Matisziw T.C., Murray A.T. et al.* Comparative Approaches for Assessing Network Vulnerability // Inter. Regional Sci. Review. 2008. V. 31.
14. *Murray A.T.* An Overview of Network Vulnerability Modeling Approaches // GeoJournal. 2013. V. 78. P. 209–221.
15. *Johansson J.* Risk and Vulnerability Analysis of Interdependent Technical Infrastructures. Addressing Socio-technical Systems. Doctoral Thesis in Industrial Automation. Department of Measurement Technology and Industrial Electrical Engineering. Lund: Lund University, 2010.
16. *Gomes T., Esposito C., Hutchison D., Kuipers F., Rak J., Tornatore M.* A Survey of Strategies for Communication Networks to Protect against Large-scale Natural Disasters // Int. Workshop on Reliable Networks Design and Modeling (RNDM). Halmstad, 2016. P. 11–22.
17. *Величко В.В., Попков Г.В., Попков В.К.* Модели и методы повышения живучести современных систем связи. М.: Горячая Линия – Телеком, 2017.
18. *Леваков А.К.* Особенности функционирования телекоммуникационных сетей следующего поколения в чрезвычайных ситуациях. М.: ИРИАС, 2012.
19. *Носков С.И., Бутин А.А., Соколова Л.Е.* Многокритериальная оценка уровня уязвимости объектов информатизации // Доклады ТУСУРа. 2014. № 2 (32). С. 137–142.
20. *Wang S., Zhang J., Duana N.* Multipleperspective Vulnerability Analysis of the Power Network // Physica A. 2018. V. 492. P. 1581–1590.
21. *Фаддеев А.М.* Оценка уязвимости энергосистем России, стран Ближнего зарубежья и Европы // Вестн. МГУ. Сер. 5. География. 2016. № 1. С. 46–53.
22. *Malashenko Y.E., Nazarova I.A., Novikova N.M., Pospelova I.I.* A Network Flow Model for Power and Energy System with Changing Capabilities // Int. J. of Public Administration. 2019. V. 42. Iss. 15–16. C. 1323–1332.
23. *Malashenko Yu.E., Nazarova I.A., Novikova N.M.* Fuel and Energy System Control at Large-scale Damages. IV. A Priori Estimates of Structural and Functional Vulnerability // J. Computer and Systems Sciences International. 2018.V. 57. № 6. P. 907–920.
24. *Royset J.O., Wood R.K.* Solving the Bi-objective Maximum-flow Network-interdiction Problem // INFORMS J. Comput. 2007. V. 19. Iss. 2. P. 175–184.
25. *Nicholson C.D., KashBarker K., Ramirez-Marquez J.E.* Flow-based Vulnerability Measures for Network Component Importance: Experimentation with Preparedness Planning // Reliability Engineering and System Safety. 2016. V. 145. P. 62–73.
26. *Кормен Т.Х., Лейзерсон Ч.И., Ривест Р.Л. и др.* Алгоритмы: построение и анализ. М.: Вильямс, 2005.