

АНАЛИЗ КРИТИЧЕСКИ ОПАСНЫХ ПОВРЕЖДЕНИЙ СЕТИ СВЯЗИ. III. ОЦЕНКИ МЕЖУЗЛОВЫХ ПОТОКОВ

© 2021 г. Ю. Е. Малашенко^a, И. А. Назарова^{a,*}

^a ФИЦ ИУ РАН, Москва, Россия

*e-mail: irina-nazar@yandex.ru

Поступила в редакцию 20.11.2020 г.

После доработки 04.12.2020 г.

Принята к публикации 25.01.2021 г.

В рамках вычислительных экспериментов анализируются изменения величин предельно допустимых потоков, которые можно передать между узлами при повреждениях сети. На начальном этапе для каждой пары вершин источник–приемник независимо определяется максимальный однопродуктовый поток. Вектор максимальных потоков используется для оценки предельных функциональных возможностей исходной, неповрежденной сети. В ходе вычислительных экспериментов последовательно рассматривается каждое повреждение из заданного множества, для всех пар источник–приемник находятся максимальные потоки в поврежденной сети. Для каждой пары узлов определяются все повреждения, при которых максимальный поток либо равен нулю, либо оказывается меньше допустимой величины. На основе полученных данных формируются диаграммы возможного ущерба для всех пар источник–приемник. Вычислительные эксперименты проводились для сетей с радиально-кольцевыми структурами и совпадающими множествами узлов. Результирующие диаграммы позволяют сравнивать и находить наиболее уязвимые пары с недоминируемыми векторными оценками ущерба.

DOI: 10.31857/S0002338821030112

Введение. Данная работа продолжает исследования, начатые в [1, 2]. В [1] оценка последствий каждого разрушения производилась по двум критериям: число разъединенных пар и/или уменьшение пропускной способности каналов связи между узлами источник–приемник. Величина ущерба вычислялась как разность максимальных значений потока между каждой парой вершин в исходной и поврежденной сети. В [2] основное внимание уделено получению гарантированных [3] оценок уязвимости сети. Для оценки ущерба от каждого повреждения определялось: общее число разъединенных пар и все направления связи, пропускная способность по которым оказывалась меньше заданного нормативного значения. Расчеты по указанным критериям позволили получить представительные векторные оценки для маркировки наиболее опасных в смысле предложенных критериев разрушающих воздействий. Предложенные в [2] методы можно рассматривать как возможные подходы к решению классической задачи исследования операций: в условиях неопределенности о намерениях нападающего оценить возможные последствия целенаправленных атак [4, 5].

В работе на модели многопользовательской сети связи [6] продолжен процесс изучения изменений предельно допустимых потоков между всеми парами узлов при разрушающих воздействиях. В качестве критического повреждения [1, 2] рассматривается подмножество ребер, при удалении которых хотя бы для одной пары узлов разрываются все возможные пути соединения. Для каждой пары вершин источник–приемник по двум критериям проводится оценка уменьшения потока при каждом повреждении из заданного множества. На первом шаге определяются все разрушающие воздействия, при которых максимально возможный поток для некоторой выделенной пары узлов становится равным нулю (первый критерий). На следующем шаге для данной пары находятся повреждения, при которых максимальный поток оказывается ниже допустимого уровня, но больше нуля (второй критерий). На основе полученных данных формируются диаграммы предельно допустимых потоков между каждой парой вершин при всех критических повреждениях из заданного множества. Граничные точки на диаграммах соответствуют наиболее уязвимым парам узлов, для них показатели потерь оказываются недоминируемыми хотя бы по

одному из критериев. Вычислительные эксперименты проводились для всех возможных комбинаций пар вершин источник-приемник с учетом направления передачи. Анализируются результаты последствий разрушающих воздействий на сетевые системы с различными структурными особенностями.

1. Математическая модель. Для описания многопользовательской сетевой системы используется математическая запись модели передачи многопродуктового потока [1, 2]. Структура сети $G(\mathbf{d})$ задается множествами $\langle V, R, U \rangle$: узлов (вершин) сети $V = \{v_1, v_2, \dots, v_n, \dots, v_N\}$; неориентированных ребер $R = \{r_1, r_2, \dots, r_k, \dots, r_E\}$. Ребро $r_k = (v_{n_k}, v_{j_k})$ соединяет вершины v_{n_k}, v_{j_k} (инцидентно вершинам v_{n_k}, v_{j_k}), которые для него служат концевыми. Предполагается, что в сети отсутствуют петли и сдвоенные ребра. Ребру r_k ставятся в соответствие две ориентированные дуги u_k, u_{k+E} прямого и обратного направления из множества ориентированных дуг $U = \{u_1, u_2, \dots, u_k, \dots, u_{2E}\}$. Дуги $\{u_k, u_{k+E}\}$ определяют направление передачи потока по ребру r_k между концевыми вершинами v_{n_k}, v_{j_k} .

Обозначим через $S(v_n)$ 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 . Состав множеств $S(v_n), T(v_n)$ однозначно определяется в ходе выполнения следующей процедуры. 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 $S(v_n)$, ориентированная дуга $u_{k+E} = (v_j, v_n)$ – *входящей* для v_n и ее номер $k + E$ помещается в список $T(v_n)$. 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 $k + E$ вносится в список исходящих дуг $S(v_j)$.

Предполагается, что в сети между любой парой узлов могут передаваться потоки разных видов. Назовем парой узлов-корреспондентов p_m упорядоченную пару вершин $p_m = (v_{s_m}, v_{t_m})$, где вершина с номером s_m является источником, а с номером t_m – стоком или приемником потока m -го вида. В настоящей работе, как и в [1, 2], в сети из N узлов рассматривается $M = N(N - 1)$ независимых, невзаимозаменяемых и равноправных потоков различных видов, которые передаются между парами узлов из множества $P = \{p_1, p_2, \dots, p_M\}$.

Пусть x_{mk} – величина потока m -го вида, который передается по дуге u_k в прямом, а $x_{m(k+E)}$ – величина потока m -го вида, который передается по дуге u_{k+E} в обратном направлении, $x_{mk} \geq 0, x_{m(k+E)} \geq 0, m = \overline{1, M}, k = \overline{1, E}$. Каждому ребру $r_k \in R$ приписывается неотрицательное число d_k , определяющее суммарный предельно допустимый поток, который можно передать по ребру r_k в обоих направлениях. В исходной сети компоненты вектора пропускных способностей – $\mathbf{d} = (d_1, d_2, \dots, d_k, \dots, d_E)$ – наперед заданные положительные числа $d_k > 0$. Вектором \mathbf{d} определяются следующие ограничения на все 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 величину потока m -го вида, который поступает в сеть в узле с номером s_m и покидает из узла с номером t_m .

Во всех узлах сети $v_n \in V, n = \overline{1, N}$, 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 входному 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 допустимых значений компонент векторов потоков $\mathbf{z} = (z_1, z_2, \dots, z_m, \dots, z_M)$:

$$\mathcal{L}(x, \mathbf{d}) = \{\mathbf{z} \geq 0 \mid (\mathbf{z}, x) \text{ удовлетворяют (1.1), (1.2)}\}. \quad (1.3)$$

2. Формирование множества структурных повреждений. В настоящей работе, как и в [1, 2], рассматриваются три типа повреждений: разрушение минимального разреза, разделяющего пару источник-приемник в неповрежденной сети, разрушение минимального разреза в сети с единичными пропускными способностями и разрушение всех ребер, инцидентных вершине.

Для построения множества повреждений первого типа для некоторой произвольной пары $p_a \in P$ решается задача поиска максимально возможного потока, который можно передать в сети $G(\mathbf{d})$ из вершины с номером s_a в вершину с номером t_a без учета всех остальных.

З а д а ч а 1. Для фиксированного a найти максимальный поток

$$z_a^0 = \max_{\mathbf{z}, x} \{z_a \mid \mathbf{z} \in \mathcal{L}(x, \mathbf{d})\}.$$

Решению задачи 1 (максимальному значению потока z_a^0) соответствует набор ребер – минимальный разрез R_a , $R_a \subset R$ [7]. Множество номеров ребер, образующих разрез R_a , обозначим

$$h(a) = \left\{ k \mid r_k \in R_a, z_a^0 = \sum_{k \in h(a)} d_k \right\},$$

здесь R_a – минимальное по суммарной пропускной способности подмножество ребер, таких, что при удалении их из сети максимальный поток из v_{s_a} в v_{t_a} становится равным нулю, т.е. в графе $G(\mathbf{d}) \setminus R_a$ между вершинами v_{s_a} и v_{t_a} нет пути.

Последовательно для всех $p_m \in P$ решаются цепочки задач 1 и формируются вектор максимальных потоков:

$$\mathbf{z}^0 = (z_1^0, z_2^0, \dots, z_m^0, \dots, z_M^0),$$

а также множество повреждений первого типа:

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

где $h(m)$ – набор номеров ребер, входящих в минимальный разрез R_m , $R_m \subset R$, $p_m \in P$. При решении задачи 1 для некоторой фиксированной пары p_a максимальному потоку z_a^0 ставится в соответствие единственный минимальный разрез $R(z_a^0)$ и набор номеров ребер $h(a)$.

Для построения критически опасных повреждений второго типа – минимальных разрезов единичной сети, в ходе вычислительного эксперимента пропускные способности всех ребер исходной сети полагаются равными единице:

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

Сеть с единичными пропускными способностями обозначим через $G(1)$, а множество достижимых потоков (1.3) – $\mathcal{L}(x, 1)$:

$$\mathcal{L}(x, 1) = \{\mathcal{L}(x, \mathbf{d}) \mid d_k = 1, k = \overline{1, E}\}.$$

Для определения минимального разреза для каждой пары $p_m \in P$ решается задача о максимальном потоке в единичной сети.

З а д а ч а 2. Для некоторой фиксированной пары p_m найти максимальный поток

$$z_m^1 = \max_{\mathbf{z}, x} \{z_m \mid \mathbf{z} \in \mathcal{L}(x, 1)\}.$$

Решение задачи 2 – максимальный целочисленный поток z_m^1 из вершины с номером s_m в вершину с номером t_m . Величина z_m^1 равна числу ребер в минимальном по суммарной пропускной

способности разрезе $R(z_m^1)$, $z_m^1 = |R(z_m^1)|$. В настоящей работе максимальному потоку z_m^1 ставится в соответствие единственный разрез $R(z_m^1)$ со списком номеров ребер

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

При удалении $R(z_m^1)$ из $G(1)$ максимальный поток z_m^1 из v_{s_m} в v_{t_m} становится равным нулю.

Множество повреждений второго типа

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

состоит из наборов номеров ребер, входящих в минимальные разрезы $R(z_m^1)$, $m = \overline{1, M}$.

Множество повреждений третьего типа

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

состоит из наборов номеров ребер, инцидентных вершине v_n :

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

где $R(v_n)$ – множество ребер, инцидентных v_n .

Для сокращения объема необходимых вычислений элементы множеств $H(\cdot)$, $Q(\cdot)$, $Y(\cdot)$ сравниваются между собой, производится удаление повторяющихся повреждений любого типа и формирование множества *уникальных* повреждений:

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

которое не содержит одинаковых элементов.

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

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

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

Задача 3. При некоторых заданных l и m найти

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

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

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

Для каждой пары $p_m \in P$ и всех $w_l \in W$ вычисляется

$$\rho(m) = \frac{\sum_{l=1}^L \xi(m, l)}{L}$$

– доля от общего числа повреждений W , при которых максимальный поток для данной пары p_m становится равен нулю.

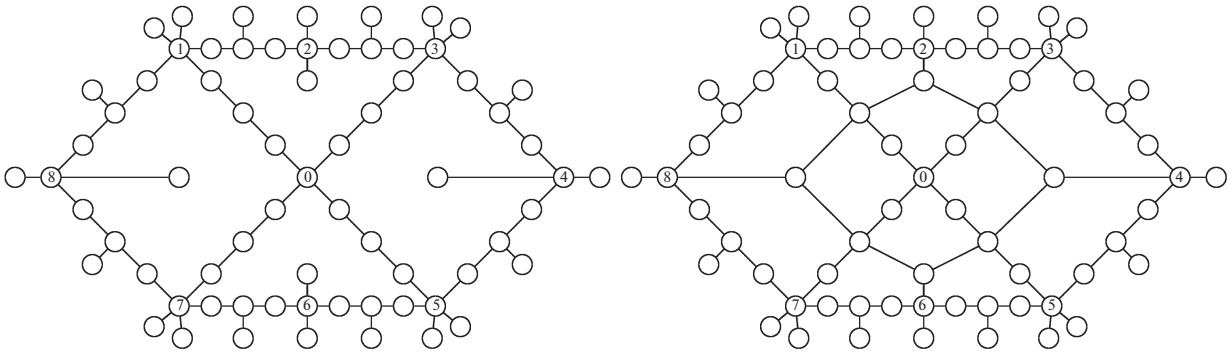


Рис. 1. Базовая и кольцевая сети

Для каждой пары p_m , для которой $z_m^0(l) > 0$ при повреждении w_l , и некоторого наперед заданного значения γ рассчитывается индикаторная функция:

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

Значение параметра γ задается априори в диапазоне $0 < \gamma < 1$. При заданном γ для некоторой пары p_m и всех повреждений из W , таких, что $z_m^0(l) > 0$, определяется

$$\varphi(m, \gamma) = \frac{\sum_{l=1}^L \eta(m, l, \gamma)}{L},$$

равная доле от общего числа повреждений из W , при которых максимальный поток для данной пары p_m становится меньше или равен заданному критическому пороговому значению γ .

На основе значений $(\rho(m), \varphi(m, \gamma))$ для всех пар $p_m \in P$ строятся диаграммы, которые позволяют оценить влияние каждого из повреждений на потоки между всеми парами вершин источник-приемник. Недоминируемые значения — точки на внешней границе диаграмм, они указывают на пары-корреспонденты, которым повреждения из W наносят наибольший ущерб хотя бы по одному из показателей.

4. Вычислительный эксперимент. Вычислительный эксперимент проводился на моделях сетевых систем, представленных на рис. 1: слева — базовая сеть, а справа — кольцевая. Пропускные способности выбирались случайным образом из отрезка $[900, 999]$ и были равны для совпадающих ребер в обеих сетях. Пропускная способность каждого из дополнительных ребер на рис. 1 справа равна 900. Число повреждений — элементов множества W — составляет 125 для базовой сети и 118 — для кольцевой. Для формирования множества W было найдено порядка 10^4 минимальных разрезов, из которых менее 100 (около 1%) оказались уникальными.

На рис. 2 слева изображена диаграмма расчетных значений $(\rho(m), \varphi(m, \gamma))$ при $\gamma = 0.6$ для базовой сети, а справа — для кольцевой. Каждый значок плюс на диаграммах относится к одной паре узлов p_m , а цифра рядом означает число пар источник-приемник с совпадающими значениями $(\rho(m), \varphi(m, \gamma))$. Большое количество точек-плюсов на оси абсцисс $\rho(m)$ относится к парам узлов, для которых $z_m^0(l) = 0$, оставшиеся значения $z_m^0(l) > 0.6$, т.е. больше заданного критического значения γ .

Для всех пар узлов оценки ущерба проводятся для всех повреждений из множества W . Значение $\rho(m)$ — относительный показатель — доля от общего числа повреждений, при которых

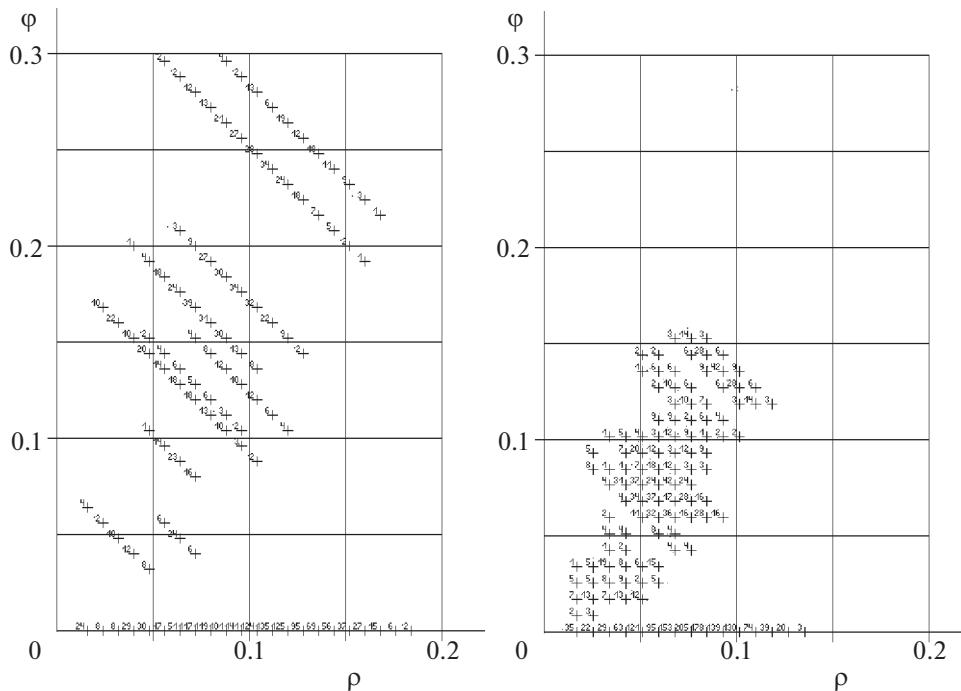


Рис. 2. Диаграмма повреждений

максимальный поток становится равным нулю для данной пары. Величина $\rho(m)$ не зависит от значений γ , а определяется структурой сети и составом множества повреждений W .

На рис. 2 значения $\phi(m, \gamma)$ по оси ординат значительно отличаются для разных сетей. В кольцевой сети больше обходных путей и максимальные потоки оказываются больше $\gamma = 0.6$ у большего числа пар-корреспондентов.

Точки-плюсы, расположенные вдоль северо-восточной границы диаграммы, соответствуют парам узлов, для которых потери потока оказываются недоминируемыми хотя бы по одному показателю ущерба $\rho(m)$ или $\phi(m, \gamma)$. Для кольцевой сети линия северо-восточной границы проходит значительно ближе к началу координат. Последнее означает, что ущерб в кольцевой сети меньше, чем в базовой, даже для самых “уязвимых” пар с наибольшими потерями.

В обеих сетях для большинства пар источник-приемник существует либо один, либо два пути соединения. На рис. 2 точки-плюсы оси абсцисс $\rho(m)$ относятся в основном к парам, имеющим один или три пути соединения. Точки на диаграмме отвечают парам узлов p_m , для которых $z_m^0(I) \leq 0.6z_m^0$, и относятся к парам с двумя возможными путями соединения. Значение $\gamma = 0.6$ выделяет все такие пары, поскольку относительные потери потока при повреждении одного из путей в среднем составляет 0.5.

На рис. 3, 4 представлены четыре диаграммы: слева для значений $\gamma = 0.673$, а справа – для $\gamma = 0.7$, на рис. 3 – для базовой сети, на рис. 4 – для кольцевой. Указанные диаграммы разительно отличаются от рис. 2 при $\gamma = 0.6$. Дело в том, что при $\gamma = 0.7$ критическими потерями считается уменьшение максимального потока на 30%, что возможно при разрушении даже одного из трех путей соединения. В результате для некоторых пар узлов, у которых $\phi(m, \gamma) = 0$ при $\gamma = 0.6$, фиксируются потери потока, и для пар p_m соответствующие точки-плюсы $\phi(m, \gamma) > 0$ оказываются недоминируемым показателем ущерба.

Для тех пар, для которых значение максимального потока в поврежденной сети

$$0.673z_m^0 \leq z_m^0(I) \leq 0.7z_m^0,$$

при $\gamma = 0.673$ не фиксируются потери потока. В результате общее число точек-плюсов на верхних ярусах диаграммы уменьшается и меняется состав (список) пар с недоминируемыми

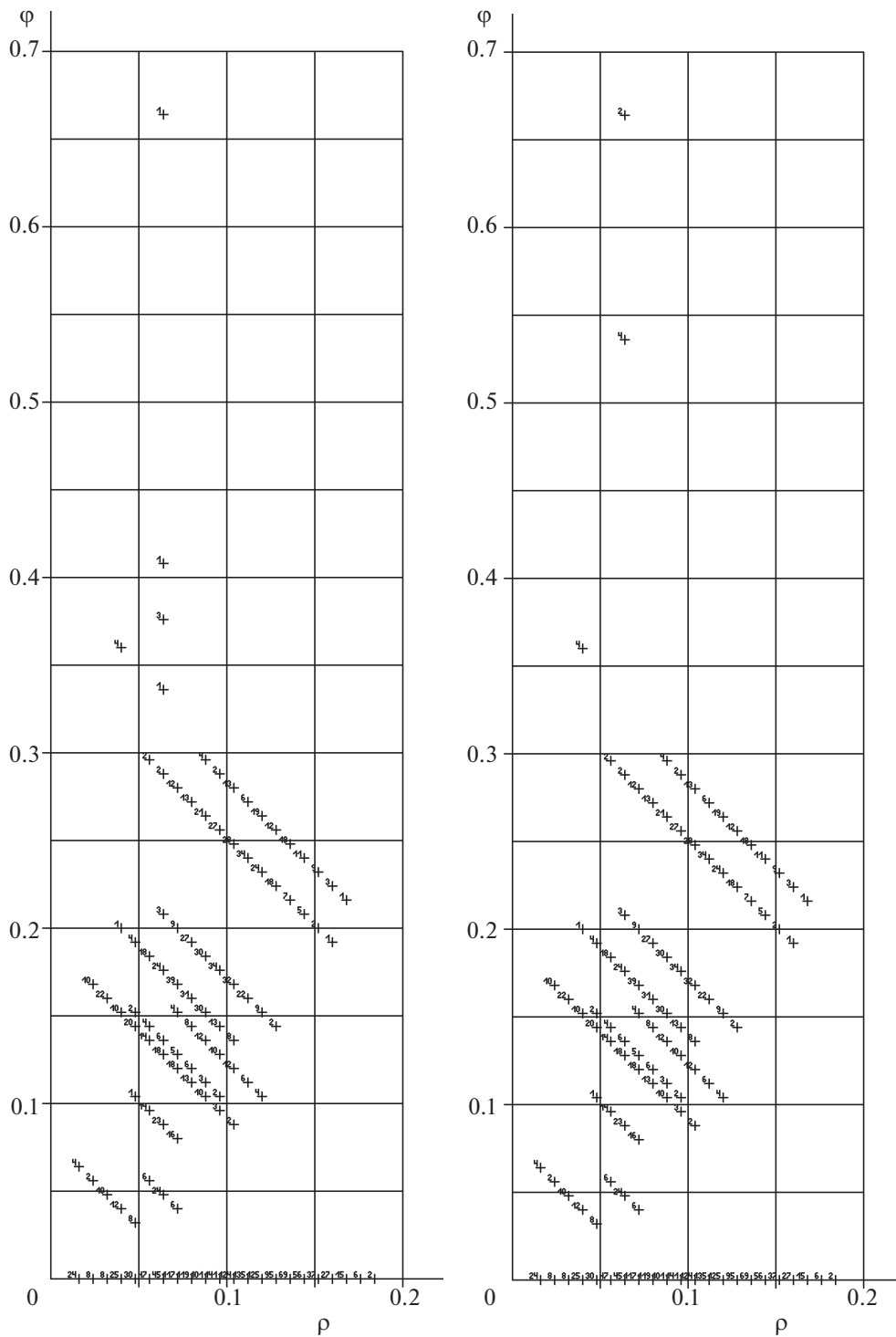


Рис. 3. Диаграмма для базовой сети

показателями ущерба. Проведенные расчеты и внешние различия диаграммы позволяют достаточно подробно анализировать последствия разрушающих воздействий. В частности, расчеты при различных γ дают возможность определять число разрушенных путей соединения. Подбрав значения γ , можно выделить группы пар-корреспондентов с разными потерями при разрушении одинакового числа путей.

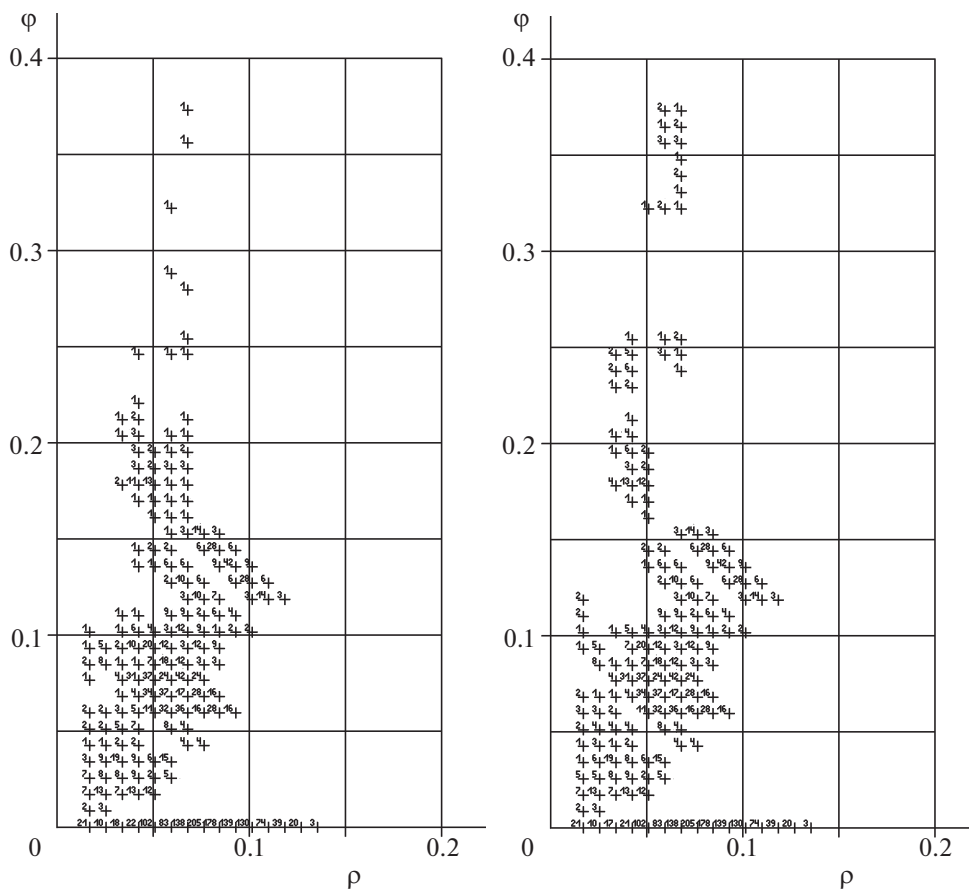


Рис. 4. Диаграмма для кольцевой сети

Заключение. В последние годы значительно возрос интерес к более предметному и комплексному анализу уязвимости сложных взаимосвязанных сетевых систем, функционирующих как единое территориально-распределенное образование [8–11]. В [9] прослеживается, как эволюционировали модели и методы исследования уязвимости и живучести: теоретико-графовые, вероятностные, эвристические, имитационные, оптимизационные и др. В [10] основное внимание уделяется специальным моделям уязвимости сетей, отмечается необходимость отдельного анализа террористических действий и/или спланированных хакерских атак, а также влияния человеческого фактора при авариях. В [11] приведен обзор возможных стратегий защиты сетей от природных катастроф.

Различные критерии и методы используются для поиска критических элементов сети [12–18]. В [12] рассматривается задача поиска множества дуг взвешенной сети, удаление которых из сети минимизирует два критерия: максимальный поток и стоимость разрушения. Парето-оптимальные решения этой задачи определяются с помощью специализированного алгоритма ветвей и границ, а также применения релаксации Лагранжа к последовательности однокритериальных задач о поиске максимального потока и минимального разреза. В [13] изучается проблема идентификации подмножества элементов (узлов, дуг, путей, клик и т.д.), удаление которых минимизирует заданную меру связности в поврежденной сети. Приводится обзор некоторых методов, в том числе использующих эвристики, математическое программирование, алгоритмы аппроксимации и подходы динамического программирования. В [14] изучаются предельные функциональные возможности многопродуктовой сети и их изменения при повреждениях сетевых элементов — минимальных разрезов трех основных типов. В частности, рассчитываются две группы количественных характеристик последствий каждого повреждения: доля разделенных пар узлов и уменьшение максимально возможного потока для каждой пары. Указанные показатели используются для двухкритериального ранжирования повреждений. Полученные агрегированные

оценки ущерба позволяют также находить критически опасные структурные повреждения сети в рамках предложенных критериев.

В [15–18] рассматривается так называемая проблема определения критических вершин, которая состоит в поиске подмножества из K вершин связного графа, удаление которых ведет к минимизации выбранного критерия связности. В [15] задача решается с использованием методов целочисленного линейного программирования, в [16] – формулируется как двухкритериальная, в [17] изучается ее NP-сложность, а также анализируются результаты проведенных вычислительных экспериментов. В [18] представлен обширный обзор по указанной теме.

Проблема уязвимости кластерных объединений при отказах различных сетевых элементов рассматривается в [19, 20]. В [19] вводится понятие среднего коэффициента кластеризации, проблема формулируется как оптимизационная, доказываемая ее NP-полнота и немонотонность, а также предлагается два алгоритма, позволяющих идентифицировать вершины, ключевые для кластерных объединений. В [20] изучается устойчивость структур кластерных связей и исследуется проблема ранжирования повреждений для заданного класса сетевых систем по трем критериям, включая мощность разреза.

В настоящей работе продолжено изучение потокового метода априорного анализа структурной неуязвимости сети при разрушениях определенного вида [1, 2]. Выбор в качестве структурных повреждений разрезов, минимальных по пропускной способности и числу ребер, а также отделяющих некоторую вершину от сети, определяется логикой исследования. Поиск наиболее уязвимых пар источник-приемник для указанных повреждений ведется по двум критериям (обнуление потока и падение потока ниже наперед заданного уровня), что позволяет заранее оценить, насколько структура сохраняет нормативную работоспособность сетевой системы после разрушения. При проведении вычислительного эксперимента использовались методы потокового программирования с полиномиальной оценкой вычислительной сложности [7, 21]. Как уже отмечалось в [2], суммарные вычислительные затраты не превышают $O(N^7)$, где N – число узлов сети. Предложенная схема проведения расчетов проста и поддается распараллеливанию, поэтому при исследовании уязвимости больших сетей могут быть использованы кластеры из персональных компьютеров с различными операционными системами.

СПИСОК ЛИТЕРАТУРЫ

1. Малашенко Ю.Е., Назарова И.А. Анализ критически опасных повреждений сети связи. I. Модель и вычислительный эксперимент // Изв. РАН. ТиСУ. 2020. № 5. С. 106–115.
2. Малашенко Ю.Е., Назарова И.А. Анализ критически опасных повреждений сети связи. II. Гарантированные оценки функциональных характеристик // Изв. РАН. ТиСУ. 2020. № 6. С. 109–119.
3. Гермейер Ю.Б. Введение в теорию исследования операций. М.: Наука, 1971.
4. Данскин Дж.М. Теория максимина и ее приложение к задачам распределения вооружения. М.: Сов. радио, 1970.
5. Cochran J.J., Cox Jr. L.A., Keskinocak P. et al. Wiley Encyclopedia of Operations Research and Management Science, 8 Volume Set. N.Y.: Wiley, 2010.
6. Малашенко Ю.Е., Назарова И.А., Новикова Н.М. Экспресс-анализ и агрегированное представление множества достижимых потоков многопродуктовой сетевой системы // Изв. РАН. ТиСУ. 2019. № 6. С. 63–72.
7. Йенсен П., Барнес Д. Потокоевое программирование. М.: Радио и связь, 1984.
8. Grubestic T.H., Matisziw T.C., Murray A.T. et al. Comparative Approaches for Assessing Network Vulnerability // Inter. Regional Sci. Review. 2008. V. 31.
9. Murray A.T. An Overview of Network Vulnerability Modeling Approaches // GeoJournal. 2013. V. 78. P. 209–221.
10. Johansson J. Risk and Vulnerability Analysis of Interdependent Technical Infrastructures. Addressing Sociotechnical Systems. Doctoral Thesis in Industrial Automation. Department of Measurement Technology and Industrial Electrical Engineering. Lund: Lund University, 2010.
11. Gomes T., Esposito C., Hutchison D. et al. 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.
12. Roysset 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.
13. Walteros J., Pardalos P. Selected Topics in Critical Element Detection // Optimization and its Applications. 2012. V. 71. P. 9–26.

14. Малащенко 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.
15. Veremyev A., Prokipyev O.A., Pasilio E.L. Critical Nodes for Distance-based Connectivity and Related Problems in Graphs // Networks. 2015. V. 66. Iss. 3. P. 170–195.
16. 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.
17. 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.
18. Lalou M., Tahraoui M.A., Kheddouci H. The Critical Node Detection Problem in Networks: a Survey // Computer Science Review. 2018. V. 28. P. 92–117.
19. Kuhnle A., Nguyen N.P., Dinh T.N. et al. Vulnerability of Clustering under Nodes Failure in Complex Networks // Social Network Analysis and Mining. 2017. V. 7. Iss. 1. P. 8–24.
20. Малащенко Ю.Е., Назарова И.А., Новикова Н.М. Анализ кластерных повреждений в сетевых системах // ЖВМиМФ, 2020. Т. 60. № 2. С. 338–348.
21. Кормен Т.Х., Лейзерсон Ч.И., Ривест Р.Л. и др. Алгоритмы: построение и анализ. М.: Вильямс, 2005.