

область применения метода направленного перебора локальных экстремумов за счет сокращения области поиска эффективных решений путем исключения мест нерационального размещения узлов.

Разработанные алгоритмы могут быть также использованы для оптимизации топологических структур централизованных систем транспорта, обслуживания, управления. Их эффективность в дальнейшем может быть повышена путем использования оценок структурных параметров сетей и итерационных алгоритмов оптимизации размещения узлов [5, 9, 10].

Литература: 1. *Вычислительные машины, системы и сети* / А.П. Пятибратов, С.Н. Беляев, Г.М. Козырева и др. М.: Финансы и статистика, 1991. 400 с. 2. *Высокопроизводительные сети*. Энциклопедия пользователя: Пер. с англ. / М. Спортак, Ф. Паппас, Э. Рензинг и др. К.: ДиаСофт, 1998. 432 с. 3. *Зайченко Ю.П., Гонта Ю.В.* Структурная оптимизация сетей ЭВМ. К.: Техника, 1986. 168 с. 4. *Болотов А.Б.* Методы и алгоритмы структурно-топологической оптимизации централизованных сетей передачи данных // Управляющие системы и машины. 1981. №5. С. 11-16. 5. *Optimierung von Telekommunikationsnetzen. Optimale Knoten / Verfasst von L. Schade.* Dresden: ZSf HSFS, 1991. 64 S. 6. *Петров Э.Г., Болотов А.Б., Бескоровайный В.В.* Алгоритм структурно-топологической оптимизации цент-

рализованных сетевых систем // Механизация и автоматизация управления. 1986. №1. С. 28-31. 7. *Петров Э.Г., Болотов А.Б., Шабанов С.В.* Алгоритм топологической оптимизации централизованных сетей передачи данных // Механизация и автоматизация управления. 1980. №4. С. 56-60. 8. *Пападимитриу Х., Стайглиц К.* Комбинаторная оптимизация. Алгоритмы и сложность: Пер. с англ. М.: Мир, 1985. 512 с. 9. *Петров Э.Г., Пискарева В.П., Бескоровайный В.В.* Территориально-распределенные системы обслуживания К.: Техника, 1992. 208 с. 10. *Бескоровайный В.В., Имангулова З.А.* Реинжиниринг топологических структур территориально распределенных систем // 5-я Международная конф. "Теория и техника передачи, приема и обработки информации". Научные труды, Харьков: ХТУРЭ, 1999. С.384-386.

Поступила в редколлегию 01.03.2000

Рецензент: д-р техн. наук Нефедов Л.И.

Бескоровайный Владимир Валентинович, канд. техн. наук, доцент кафедры системотехники ХТУРЭ. Научные интересы: структурный синтез ТРС; теория выбора решений. Адрес: Украина, 61166, Харьков, пр. Ленина, 14, тел. 40-93-06.

Имангулова Зульфия Алиевна, аспирантка кафедры системотехники ХТУРЭ. Научные интересы: структурно-топологическая оптимизация ИВС. Адрес: Украина, 61166, Харьков, ул. ак. Ляпунова, 9, кв. 66, тел. 19-55-43.

УДК 681.3+681.5:007

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В ДИСКРЕТНОМ КАНАЛЕ НА ОСНОВЕ ПОМЕХОУСТОЙЧИВЫХ К НЕСИММЕТРИЧНЫМ НЕРЕГУЛЯРНЫМ ВИРТУАЛЬНЫМ ПОМЕХАМ АЛГОРИТМОВ ПОИСКА ТОЧКИ С ХАРАКТЕРНЫМ ПРИЗНАКОМ

*АЛИПОВ Н.В., АЛИПОВ И.Н., БЕЛЯЕВ С.А.,
РЕБЕЗЮК Л.Н.*

Строятся помехоустойчивые алгоритмы поиска точки с характерным признаком в условиях несимметричного нерегулярного воздействия виртуальной последовательности, определяющие функционирование дискретных автоматов систем защиты информации.

Известно [1], что виртуальная помеха описывается такими параметрами: длительностью (l), интервалом между двумя соседними выбросами (импульсами) виртуальной помехи (h) и амплитудой помехи (a). Каждый из этих параметров может быть случайной либо неслучайной величиной. В работе рассматриваются такие виртуальные помехи (последовательности), у которых только один параметр l является случайной величиной. Поскольку пара-

метр h — неслучайная величина, то в виртуальной последовательности импульсы отделены друг от друга интервалами $h \cdot \Delta t$ (Δt — длительность шага алгоритма поиска точки с характерным признаком). На этом основании можно утверждать: длительность выброса не может быть меньше Δt . Будем в дальнейшем считать, что случайная величина l принадлежит диапазону $[l_1, l_2]$, где l_1 — минимальное значение параметра l ; l_2 — максимальное значение параметра l .

Любой алгоритм поиска точки [1] характеризуется: длительностью поиска (количеством шагов алгоритма) i ; количеством точек эксперимента, исполняемого на любом шаге алгоритма, k ; видом виртуальной последовательности (описанная в работе [2] виртуальная последовательность называется $A_{1,3}$ — последовательностью, критерием оптимальности (используется минимаксный критерий [3]). В этих условиях требуется, на основе принципа "пересечения" [4] и принципа "повторных" сравнений, точку x с характерным признаком за i шагов алгоритма заключить в интервал неопределенности наименьшей длины [3].

С учетом сказанного выполним эксперимент на первом шаге алгоритма. Расположим на первом шаге алгоритма в исходном интервале $(0, l)k$ точек эксперимента. По итогам выполнения первого шага алгоритма может возникнуть один из исходов:

$$a) \quad x(t_1) \in [0, x_1^1]; \quad б) \quad x_1 \in [x_q^1, x_{q+1}^1),$$

где $x(t_1)$ – аддитивная сумма координаты точки с характерным признаком и амплитуда виртуальной последовательности; t_1 – момент времени, соответствующий завершению первого шага алгоритма;

$q = \overline{1, k}$; $x_{k+1}^1 = 1$ – координата q -й точки первого эксперимента.

Будем считать, что алгоритм поиска точки x за i своих шагов разбивает первоначальный интервал неопределенности на $\phi_{1,3}^{h,l_1,l_2,a}(i, k)$ равных частей.

Для исхода а) устанавливаем: $x \in [0, x_1^1]$. Поскольку в распоряжении алгоритма осталось $(i-1)$ шагов, то за это количество шагов полуоткрытый интервал неопределенности $[0, x_1^1]$ будет разбит на $\phi_{1,3}^{h,l_1,l_2,a}(i-1, k)$ равных частей. Из этого утверждения следует:

$$x_1^1 = \delta \phi_{1,3}^{h,l_1,l_2,a}(i-1, k), \quad (1)$$

где δ – дискретность преобразования по амплитуде.

Для исхода б) необходимо применить принцип пересечения, на основании которого устанавливаем:

$$x \in [x_q^{1,1}, x_{q+1}^1];$$

$$x_q^{1,1} = \begin{cases} x_q^1 - a\delta, x_q^1 - a\delta \geq 0; \\ 0, \text{ в противном случае,} \end{cases}$$

и применить смешанную стратегию[4]:

$$x_1^2 = x_q^1; x_\rho^2 \in [x_q^1, x_{q+1}^1];$$

$$\rho = \overline{2, (k-1)}; \quad (2)$$

$$x_k^2 = x_{q+1}^1.$$

По итогам выполнения второго шага алгоритма может возникнуть один из исходов:

$$в_1) x(t_1 + \Delta t) < x_1^2;$$

$$в_2) x(t_1 + \Delta t) \in [x_\rho^2, x_{\rho+1}^2];$$

$$в_3) x(t_1 + \Delta t) > x_k^2;$$

Для исхода $в_1)$ характерно то, что виртуальная последовательность, которая проявляется на первом шаге алгоритма, не будет проявляться на последующих $(h-1)$ -м шагах. На этих шагах алгоритма следует применить классический алгоритм поиска в новом полуоткрытом интервале неопреде-

лённости $[x_q^{1,1}, x_q^1]$. Затем на последующих l_3 шагах алгоритма, где $l_3 \in [l_1, l_2]$, ее действие снова будет проявляться. Эти шаги следует пропустить. Исходя из такой особенности проявления виртуальной последовательности, необходимо определять шаги алгоритма, на которых действие виртуальной последовательности заканчивается.

Как нетрудно заметить, действие виртуальной последовательности начнется на $(h+2)$ -м шаге алгоритма. Начиная с этого шага и кончая $(h+l_1+1)$ -м шагом, в обязательном порядке будет наблюдаться проявление виртуальной последовательности. На этих шагах алгоритма поиск координаты точки с характерным признаком не выполняется. На следующем $(h+l_1+2)$ -м шаге действие виртуальной последовательности может прекратиться (длительность помехи случайная величина, принадлежащая диапазону $[l_1, l_2]$). Поэтому на этом и последующих $(l_2 - l_1)$ шагах применяют смешанную стратегию:

$$x_{\rho_2}^{h+l_1+z+1} \in [x_{\rho_1}^{h+1}, x_{\rho_1+1}^{h+1});$$

$$\rho_2 = \overline{1, k-1}; \quad (3)$$

$$x_k^{h+l_1+z+1} = x_q^1; z = \overline{1, l_2 - l_1},$$

где $[x_{\rho_1}^{h+1}, x_{\rho_1+1}^{h+1})$ – полуоткрытый интервал неопределённости, выделенный классическим алгоритмом поиска на $(h+1)$ -м шаге и принадлежащий полуоткрытому интервалу $[x_q^{1,1}, x_q^1]$, а также проверяют истинность предиката:

$$P\{x_k^{h+l_1+z+1} \geq x(t_1 + \Delta t(h+l_1+z))\}. \quad (4)$$

Если соотношение (4) не будет истинным, то, не изменяя координат точек эксперимента, выполняют следующий шаг и так далее. Первый шаг, на котором соотношение (4) станет истинным, будет шагом окончания действия виртуальной последовательности. Истинность предиката (4) будет свидетельствовать также о том, что на $(h+l_1+z+1)$ -м шаге алгоритма амплитуда виртуальной последовательности стала равна нулю, следовательно, результаты этого шага алгоритма являются истинными. Поскольку в полуоткрытом интервале неопределённости выделенного на $(h+1)$ -м шаге алгоритма были размещены $(k-1)$ точки эксперимента, то он будет разбит на k равных частей. На последующих $(h-1)$ -м шагах алгоритма амплитуда виртуальной последовательности также будет равна нулю. Поэтому на этих шагах следует применять классический алгоритм поиска, который на каждом шаге разбивает исходный интервал неопределённости на $(k+1)$ равные части.

Применяя на последующих шагах алгоритма описанную схему поиска точки x с характерным признаком, исходный полуоткрытый интервал неопределенности $[x_q^{l_1}, x_q)$ в наихудшем случае можно разбить на $\bar{\varphi}_{1,3}^{h,l_1,l_2,a}(i_1, k)$, а в наилучшем — на $\bar{\varphi}_{1,3}^{h,l_1,l_2,a}(i_2, k)$ равных частей, где

$$i_1 = \alpha_1(h-1) + \alpha_2 + \alpha_3; \quad i_2 = \bar{\alpha}_1(h-1) + \bar{\alpha}_2 + \alpha_3;$$

$$\bar{\varphi}_{1,3}^{h,l_1,l_2,a}(i_1, k) = (k+1)^{\alpha_1(h-1)} \cdot k^{\alpha_3} \cdot (k+1)^{\alpha_2};$$

$$\bar{\varphi}_{1,3}^{h,l_1,l_2,a}(i_2, k) = (k+1)^{\bar{\alpha}_1(h-1)} \cdot k^{\bar{\alpha}_3} \cdot (k+1)^{\bar{\alpha}_2};$$

$$\alpha_1 = \begin{cases} \frac{i-1}{l_2+h}, (i-1) \bmod(l_2+h) = 0; \\ \left\lfloor \frac{i-1}{\alpha_2+h} \right\rfloor, (i-1) \bmod(l_2+h) \neq 0; \end{cases}$$

$$\alpha_2 = \begin{cases} 0, (i-1) \bmod(l_2+h) = 0; \\ (i-1) \bmod(l_2+h) - 1, \\ (i-1) \bmod(l_2+h) \leq h; \\ h-1, (i-1) \bmod(l_2+h) > h; \end{cases} \quad (5)$$

$$\alpha_3 = \begin{cases} \alpha_1 - 1, (i-1) \bmod(l_2+h) = 0; \\ \alpha_1, (i-1) \bmod(l_2+h) \neq 0; \end{cases}$$

$$\bar{\alpha}_1 = \begin{cases} \frac{i-1}{l_1+h}, (i-1) \bmod(l_1+h) = 0; \\ \left\lfloor \frac{i-1}{l_1+h} \right\rfloor, (i-1) \bmod(l_1+h) \neq 0; \end{cases}$$

$$\bar{\alpha}_2 = \begin{cases} 0, (i-1) \bmod(l_1+h) = 0; \\ (i-1) \bmod(l_1+h) - 1, \\ (i-1) \bmod(l_1+h) \leq h; \\ h-1, (i-1) \bmod(l_1+h) > h; \end{cases}$$

$$\bar{\alpha}_3 = \begin{cases} \bar{\alpha}_1 - 1, (i-1) \bmod(l_1+h) = 0; \\ \bar{\alpha}_1, (i-1) \bmod(l_1+h) \neq 0; \end{cases}$$

Если возникнет исход v_3 , то это будет означать, что проявление виртуальной последовательности началось на втором шаге алгоритма и может окончиться на одном из шагов алгоритма (смотри параметры виртуальной последовательности): на $(l_1+1)-m, (l_1+2)-m, \dots, (l_2+1)-m$.

Поэтому, как и для исхода v_1 , чтобы обнаружить момент окончания действия виртуальной последовательности, применяют такую же схему: пропускают (l_1-1) -шаг алгоритма, затем на последующих шагах применяют смешанную стратегию:

$$x_{p_3}^{l_1+z+1} \in [x_q^1, x_{q+1}^1), p_3 = \overline{l, k-1};$$

$$x_k^{l_1+z+1} = x_{q+1}^1, z = \overline{l, l_2-l_1}$$

и проверяют истинность предиката

$$P\{x_k^{l_1+z+1} \geq x(t_1 + \Delta t \cdot (l_1 + z))\}. \quad (6)$$

Шаг алгоритма, на котором предикат (6) будет истинным, является шагом окончания действия виртуальной последовательности. На последующих $(h-1)$ шагах применяют классический алгоритм поиска точки x с характерным признаком.

Такая схема поиска позволяет разбить исходный полуоткрытый интервал неопределённости $[x_q^1, x_{q+1}^1)$ в наихудшем случае на $\bar{\varphi}_{1,3}^{h,l_1,l_2,a}(i_3, k)$, а в наилучшем — на $\bar{\varphi}_{1,3}^{h,l_1,l_2,a}(i_4, k)$ равных частей, где $i_3 = \alpha_4(h-1) + \alpha_5 + \alpha_6$;

$$i_4 = \bar{\alpha}_4(h-1) + \bar{\alpha}_5 + \bar{\alpha}_6;$$

$$\alpha_4 = \begin{cases} \frac{i-l_2-1}{l_2+h}, (i-l_2-1) \bmod(l_2+h) = 0; \\ \left\lfloor \frac{i-l_2-1}{l_2+h} \right\rfloor, (i-l_2-1) \bmod(l_2+h) \neq 0; \end{cases}$$

$$\alpha_5 = \begin{cases} 0, (i-l_2-1) \bmod(l_2+h) = 0; \\ (i-l_2-1) \bmod(l_2+h) - 1, \\ (i-l_2-1) \bmod(l_2+h) \leq h; \\ h-1, (i-l_2-1) \bmod(l_2+h) > h; \end{cases}$$

$$\alpha_6 = \begin{cases} \alpha_4 - 1, (i-l_2-1) \bmod(l_2+h) = 0; \\ \alpha_4, (i-l_2-1) \bmod(l_2+h) \neq 0; \end{cases} \quad (7)$$

$$\bar{\alpha}_4 = \begin{cases} \frac{i-l_1-1}{l_2+h}, (i-l_1-1) \bmod(l_1+h) = 0; \\ \left\lfloor \frac{i-l_1-1}{l_2+h} \right\rfloor, (i-l_1-1) \bmod(l_1+h) \neq 0; \end{cases}$$

$$\bar{\alpha}_5 = \begin{cases} 0, (i-l_1-1) \bmod(l_1+h) = 0; \\ (i-l_1-1) \bmod(l_1+h) - 1, \\ (i-l_1-1) \bmod(l_1+h) \leq h; \\ h-1, \bmod(l_1+h) > h; \end{cases}$$

$$\bar{\alpha}_6 = \begin{cases} \bar{\alpha}_4 - 1, (i-l_1-1) \bmod(l_1+h) = 0; \\ \bar{\alpha}_4, (i-l_1-1) \bmod(l_1+h) \neq 0; \end{cases}$$

$$\bar{\varphi}_{1,3}^{h,l_1,l_2,a}(i_3, k) = (k+1)^{\alpha_4(h-1)} \cdot k^{\alpha_6} \cdot (k+1);$$

$$\bar{\varphi}_{1,3}^{h,l_1,l_2,a}(i_4, k) = (k+1)^{\bar{\alpha}_4(h-1)} \cdot k^{\bar{\alpha}_6} \cdot (k+1)^{\bar{\alpha}_5}.$$

Если же на втором шаге алгоритма возникает исход типа v_2), то применяется принцип “пересечения”, на основании которого устанавливаем $x \in [x_p^{2,1}, x_{p+1}^2]$,

$$\text{где } x_p^{2,1} = \begin{cases} x_p^{2,1} - a \cdot \delta, x_p^2 - a \cdot \delta \leq x_q^{1,1}; \\ x_q^{1,1}, \text{ в противном случае,} \end{cases}$$

и на третьем шаге снова применяем смешанную стратегию типа (2).

Анализ возможных исходов, возникающих по итогам выполнения второго шага, показывает: для исходов v_1), v_3) выявляется действие виртуальной последовательности, что позволяет построить логическую схему алгоритма, начиная с $(i-3)$ шага и кончая i -м шагом; для исхода v_2) построить логическую схему алгоритма пока не удаётся. Предположим, что исход типа v_2) возникает на первых j -х шагах алгоритма. Тогда, как известно, на следующем $(j+1)$ -м шаге, в случае $(j+1 \leq l_2)$, снова применяем смешанную стратегию вида (2). По итогам выполнения $(j+1)$ -го шага алгоритма может возникнуть один из исходов типа v_1), v_2) и v_3).

В случае исхода типа v_1) будем иметь такие соотношения для параметров $\alpha_1, \alpha_2, \alpha_3$:

$$\alpha_1 = \begin{cases} \frac{i-j}{l_2+h}, (i-j) \bmod (l_2+h) = 0; \\ \left\lfloor \frac{i-j}{l_2+h} \right\rfloor, (i-j) \bmod (l_2+h) \neq 0; \end{cases}$$

$$\alpha_2 = \begin{cases} 0, (i-j) \bmod (l_2+h) = 0; \\ (i-j) \bmod (l_2+h) - 1, \\ (i-j) \bmod (l_2+h) \leq h; \\ h-1, (i-j) \bmod (l_2+h) > h; \end{cases} \quad (8)$$

$$\alpha_3 = \begin{cases} \alpha_1 - 1, (i-j) \bmod (l_2+h) = 0; \\ \alpha_1, (i-j) \bmod (l_2+h) \neq 0; \end{cases}$$

Подобные соотношения справедливы и для параметров $\bar{\alpha}_1, \bar{\alpha}_2, \bar{\alpha}_3$.

В случае исхода типа v_3) для параметров $\alpha_4, \alpha_5, \alpha_6$ будут справедливы такие соотношения:

$$\alpha_4 = \begin{cases} \frac{i-l_2-j}{l_2+h}, (i-l_2-j) \bmod (l_2+h) = 0; \\ \left\lfloor \frac{i-l_2-j}{l_2+h} \right\rfloor, (i-l_2-j) \bmod (l_2+h) \neq 0; \end{cases}$$

$$\alpha_5 = \begin{cases} 0, (i-l_2-j) \bmod (l_2+h) = 0; \\ (i-l_2-j) \bmod (l_2+h) - 1, \\ (i-l_2-j) \bmod (l_2+h) \leq h; \\ h-1, (i-l_2-j) \bmod (l_2+h) > h; \end{cases} \quad (9)$$

$$\alpha_6 = \begin{cases} \alpha_4 - 1, (i-l_2-j) \bmod (l_2+h) = 0; \\ \alpha_4, (i-l_2-j) \bmod (l_2+h) \neq 0; \end{cases}$$

Подобные соотношения имеют место и для параметров $\bar{\alpha}_4, \bar{\alpha}_5, \bar{\alpha}_6$.

Если же исход типа v_2) возник на первых j -х шагах алгоритма и имеют место соотношения:

$$h \leq l_2, (j+1) > l_2 \text{ или } h > l_2, (j+i) > h,$$

то это означает, что амплитуда виртуальной последовательности мала или равна нулю и не может сказаться на результатах экспериментов. Поэтому к выделенному на j -м шаге алгоритма полуоткрытому интервалу неопределённости применяют помехоустойчивый $(i-j)$ -шаговый алгоритм поиска, который разобьёт этот интервал на $\varphi_{1,3}^{h,l_1,l_2,a}(i-j, k)$ равных частей.

Анализ возможных исходов, возникающих в процессе поиска точки с характерным признаком, показывает, что полуоткрытый интервал неопределённости $[x_q^1, x_{q+1}^1]$, выделенный на первом шаге алгоритма, будет разбит на

$$\begin{aligned} \bar{\varphi}_{1,3}^{h,l_1,l_2,a}(i-j, k) &= \\ &= (k-1)^j \cdot \varphi_{1,3}^{h,l_1,l_2,a}(i-j, k) \end{aligned} \quad (10)$$

равные части.

На основании соотношений (1), (6), (7), (10) устанавливаем такую закономерность:

$$\begin{aligned} \varphi_{1,3}^{h,l_1,l_2,a}(i, k) &= \\ &= \varphi_{1,3}^*(i_3, k) + k \cdot \bar{\varphi}_{1,3}^{h,l_1,l_2,a}(i-j, k), \end{aligned} \quad (11)$$

где $\varphi_{1,3}^*(i_3, k)$ определяем из соотношений:

$$h = \max \left\{ \frac{x_1^1}{\varphi_{1,3}^{h,l_1,l_2,a}(i-1, k)}, \frac{x_1^1 - x_1^{1,1}}{\varphi_{1,3}^{h,l_1,l_2,a}(i-j, k)} \right\};$$

$$\varphi_{1,3}^{h,l_1,l_2,a}(i_3, k) \in [\varphi_{1,3}^{h,l_1,l_2,a}(i_3, k), \varphi_{1,3}^{h,l_1,l_2,a}(i_4, k)];$$

$$\varphi_{1,3}^*(i_3, k) = \begin{cases} \varphi_{1,3}^{h,l_1,l_2,a}(i-1, k), h = \frac{x_1^1}{\varphi_{1,3}^{h,l_1,l_2,a}(i-1, k)}; \\ \varphi_{1,3}^{h,l_1,l_2,a}(i_3, k), h = \frac{x_1^1 - x_1^{1,1}}{\varphi_{1,3}^{h,l_1,l_2,a}(i_3, k)}. \end{cases}$$

Приведенные логические схемы решения исходов, возникающих в процессе поиска точки с характерным признаком, правила формирования нового интервала неопределённости обосновывает следующий алгоритм поиска:

1-й шаг: выбрать точки эксперимента на основании соотношений:

$$x_1^1 = \delta \cdot \varphi^*(i_3, k);$$

$$x_q^1 = x_1^1 + \delta(q-1) \cdot \varphi_{1,3}^{-h, l_1, l_2, a}(i - \beta, k);$$

$$q = \overline{2, k}; \beta = \begin{cases} 1, l > h; \\ h, h > l. \end{cases}$$

2-й шаг: если в результате выполнения первого шага алгоритма возникает исход типа а), то разрешить его согласно соотношению (1); если же возникает исход типа б), то применить к этому исходу принцип “пересечения” и смешанную стратегию, задаваемую соотношениями (2).

3-й шаг: если по итогам выполнения второго шага алгоритма возникают исходы типа v_1) и v_3), то разрешить их согласно логическим схемам, описываемым соотношениями (5), (8), (9); если же на втором шаге алгоритма сформирован исход типа v_2), то к вновь выделенному полуоткрытому интервалу неопределённости применить принцип “пересечения” и смешанную стратегию типа (2).

Последующие шаги алгоритма 4-й, 5-й, ..., l_1 -й совершаются таким же образом.

(l_1+1) -й шаг: если по итогам выполнения l_1 -го шага возникает исход типа v_1), то его разрешают на основании соотношений (4), (5), (8); если возникает исход типа v_3), то его разрешают, применяя соотношения (6), (7), (9); если же возникает исход типа v_2), то к вновь выделенному полуоткрытому интервалу неопределённости применить принцип “пересечения” и смешанную стратегию типа (2).

Последующие (l_1+2) , (l_1+3) , ..., l_2 шаги совершаются таким же образом:

(l_2+1) -й шаг: если при выполнении l_2 -го шага алгоритма возникает исход v_1), то его разрешают на основании соотношений (4), (5), (8); если по итогам выполнения l_2 -го шага возникает исход типа v_3), то его разрешают на основании соотношений (6), (7), (9); если возникает исход типа v_2), то к вновь выделенному полуоткрытому интервалу неопределённости применяют помехоустойчивый $(i-l_2)$ -шаговый алгоритм поиска точки с характерным признаком.

Рассмотрим один частный случай, для которого характерно то, что $k = 1, l_1 = 1, l_2 = 2, h > l_2$, амплитуда выброса виртуальной последовательности значительно превосходит длину исходного интервала неопределённости.

Пусть единственная точка первого эксперимента совпадает с точкой $x_1^1 \in [0, 1]$; совершаем первый шаг алгоритма поиска. Тогда, как нам известно, по итогам первого шага может быть сформирован один из исходов типа а) либо б).

Для исхода а) (см. соотношение (1))

$$x_1^1 = \delta \varphi_{1,3}^{h, l_1, l_2, a}(i - 1, k).$$

Для исхода б) точку эксперимента выбираем согласно соотношению $x_1^2 \in (x_1^1, 1)$.

По итогам выполнения второго шага алгоритма может быть сформирован исход типа а). В этом случае на третьем шаге алгоритма выбирается такая точка эксперимента:

$$x_1^3 = x_1^1. \quad (12)$$

В результате выполнения третьего шага алгоритма может возникнуть исход типа а) либо б).

Для исхода типа а) характерно действие виртуальной последовательности на первом шаге алгоритма, на втором шаге проявление её окончилось и она ещё не будет наблюдаться на $(h-2)$ шагах алгоритма. В таком случае на этих шагах применяют классический алгоритм поиска, затем используют описанную нами ранее логическую схему (пропускают l_3 шага ($l_3 \in [l_1, l_2]$), затем снова используют классический алгоритм поиска и т.д.). Положим, что в результате такой комбинации поисковых процедур полуоткрытый интервал неопределённости будет разбит на $\psi_{1,3}(i-3, k)$ равных частей.

Для исхода б) характерно то, что виртуальная последовательность не проявлялась на первых трёх шагах алгоритма. По этой причине $x \in [x_1^1, x_1^2]$ и этот полуоткрытый интервал неопределённости будет разбит на $\varphi_{1,3}^{h, l_1, l_2, a}(i-3, k)$ равных частей.

В том случае, когда по итогам выполнения второго шага алгоритма возникает исход б), точку эксперимента на третьем шаге алгоритма выбирают согласно соотношению:

$$x_1^3 \in (x_1^2, 1). \quad (13)$$

В результате выполнения третьего шага алгоритма может появиться исход а) либо б). В случае, когда возникает исход типа а), точку следующего четвертого эксперимента выбирают таким образом:

$$x_1^4 = x_1^1.$$

Если по итогам четвертого шага будет сформирован исход типа а), то это будет свидетельствовать о действии виртуальной последовательности на первых шагах алгоритма и $x \in [0, x_1^1]$. Действуя на этом полуоткрытом интервале неопределённости относительно x классическим алгоритмом на первых $(h-2)$ -х шагах алгоритма, затем пропуская последующие l_3 шагов алгоритма и т.д., разобьём полуоткрытый интервал неопределённости на $\psi_{1,3}(i-3, k)$ равных частей. Если по итогам выполнения четвертого эксперимента в точке $x_1^4 = x_1^1$ формируется исход типа б), то это будет свидетельствовать о том, что $x \in [x_1^1, x_1^2]$ либо $x \in [x_1^2, x_1^3]$.

Для установления однозначного ответа на эту ситуацию пятый эксперимент необходимо совершить в точке $x_1^5 = x_1^2$. Если при этом возникает исход типа а), то это свидетельствует о том, что виртуальная последовательность действовала на втором шаге алгоритма и точка с характерным признаком находится в полуоткрытом интервале $[x_1^1, x_1^2)$. Этот полуоткрытый интервал будет разбит на $\psi_{1,3}(i-5, k)$ равных частей (по аналогии с исходом а), возникающих при расположении точки третьего эксперимента в точке x_1^1 .

Если по итогам выполнения пятого шага формируется исход типа б), то это свидетельствует о том, что $x \in [x_1^2, x_1^3)$ и проявление виртуальной последовательности не обнаружено. По этой причине на этом полуоткрытом интервале действует помехоустойчивый (i-5)-шаговый алгоритм поиска, который разбивает его за это количество шагов на $\phi_{1,3}^{h,l_1,l_2,a}(i-5, k)$ равных частей.

Если при выполнении третьего эксперимента в одной из точек $x_1^3 \in (x_1^2, 1)$ возникает исход типа б), то это будет свидетельствовать о том, что на первом шаге алгоритма амплитуда виртуальной последовательности равнялась нулю и по этой причине $x \in [x_1^1, 1)$.

Следующий четвертый эксперимент для данного исхода выполняется в точке $x_1^4 \in (x_1^3, 1)$.

Этот эксперимент приводит к формированию исхода типа а) либо б).

Для исхода типа а) пятый эксперимент выполняется в точке $x_1^5 = x_1^2$. В результате выполнения этого эксперимента может быть сформирован исход типа а) либо б). Для исхода типа а) характерно действие виртуальной последовательности на втором и третьем шагах алгоритма. На этом основании устанавливаем $x \in [x_1^1, x_1^2)$. Этот полуоткрытый интервал неопределённости за оставшиеся (i-5) шагов алгоритма классическим алгоритмом поиска с пропуском l_3 шагов алгоритма ($l_3 \in [1, l_2]$) будет разбит на $\psi_{1,3}(i-5, k)$ равных частей. Для исхода типа б) нельзя однозначно утверждать, какому из двух интервалов $[x_1^2, x_1^3)$, $[x_1^3, x_1^4)$ принадлежит точка x с характерным признаком. Для установления истинности в отношении принадлежности x к одному из интервалов неопределённости необходимо выполнить шестой эксперимент в точке $x_1^6 = x_1^3$.

Как нам известно, при этом тоже может появиться один из исходов типа а) либо б).

Для исхода типа а) характерно то, что виртуальная последовательность действовала на третьем шаге алгоритма. На этом основании устанавливаем

$$x \in [x_1^2, x_1^3).$$

Этот полуоткрытый интервал за оставшиеся (i-6) шагов классическим алгоритмом поиска с пропуском шагов, на которых действует виртуальная

последовательность, будет разбит на $\psi_{1,3}(i-6, k)$ равных частей.

Для исхода типа б) проявление виртуальной последовательности не обнаружено. На этом основании устанавливаем $x \in [x_1^3, x_1^4)$. Этот полуоткрытый интервал неопределённости за оставшиеся (i-6) шагов будет разбит помехоустойчивым алгоритмом на $\phi_{1,3}^{h,l_1,l_2,a}(i-6, k)$ равных частей.

Для четвертого эксперимента, совершенного в точке $x_1^4 \in (x_1^3, 1)$, при формировании исхода типа б) на первых двух шагах проявление виртуальной последовательности не наблюдалось. По этой причине справедливым будет соотношение $x \in [x_1^2, 1)$. Для данного исхода пятый эксперимент выполняется в точке $x_1^5 \in (x_1^4, 1)$.

Если при этом возникает исход типа а), то следующий эксперимент выполняется в точке $x_1^6 = x_1^3$, на основании которого при формировании исхода а) устанавливаем $x \in [x_1^2, x_1^3)$ и этот интервал будет разбит на $\psi_{1,3}(i-6, k)$ равных частей. Если при выполнении шестого эксперимента возникает исход типа б), то седьмой эксперимент выполняем в точке $x_1^7 = x_1^4$. В этом случае при появлении исхода типа а) устанавливаем $x \in [x_1^3, x_1^4)$. Этот полуоткрытый интервал неопределённости будет разбит, как нам уже известно, на $\psi_{1,3}(i-7, k)$ равных частей. Если же возникает исход типа б), то будет справедливым соотношение $x \in [x_1^4, x_1^5)$. Этот полуоткрытый интервал неопределённости будет разбит на $\phi_{1,3}^{h,l_1,l_2,a}(i-7, k)$ равных частей.

Если по итогам выполнения эксперимента в точке $x_1^5 \in (x_1^4, 1)$ возникает исход типа б), то это будет свидетельствовать, что $x \in [x_1^3, 1)$.

Следующий, шестой эксперимент в этом случае выполняется в точке $x_1^6 \in (x_1^3, 1)$.

Проведенный детальный анализ исходов, возникающих в процессе поиска, позволяет установить закономерность распределения точек экспериментов.

Для точки x_1^1 характерны такие соотношения:

$$x_1^1 = \delta \cdot \phi_{1,3}^{h,l_1,l_2,a}(i-1, k);$$

$$x_1^1 = \delta \cdot \psi_{1,3}(i-3, k);$$

$$x_1^1 = \delta \cdot \psi_{1,3}(i-4, k);$$

На основании минимального критерия устанавливаем:

$$x_1^1 = \delta \cdot \min \left\{ \phi_{1,3}^{h,l_1,l_2,a}(i-1, k), \psi_{1,3}(i-3, k), \psi_{1,3}(i-4k) \right\}. \quad (14)$$

Для точки x_1^2 справедливы следующие соотношения:

$$x_1^2 = x_1^1 + \delta \cdot \varphi_{1,3}^{h,l_1,l_2,a}(i-3,k);$$

$$x_1^2 = x_1^1 + \delta \cdot \psi_{1,3}(i-5,k).$$

На основании минимального критерия устанавливаем:

$$x_1^2 = x_1^1 + \delta \cdot \min \{ \varphi_{1,3}^{h,l_1,l_2,a}(i-3,k), \psi_{1,3}(i-5,k) \}. \quad (15)$$

Для точки x_1^3 имеют место такие равенства:

$$x_1^3 = x_1^2 + \delta \cdot \varphi_{1,3}^{h,l_1,l_2,a}(i-5,k);$$

$$x_1^3 = x_1^2 + \delta \cdot \psi_{1,3}(i-6,k).$$

Согласно минимальному критерию будем иметь:

$$x_1^3 = x_1^2 + \delta \cdot \min \{ \varphi_{1,3}^{h,l_1,l_2,a}(i-5,k), \psi_{1,3}(i-6,k) \}. \quad (16)$$

Для точек всех последующих экспериментов справедливо такое выражение:

$$x_1^j = x_1^{j-1} + \delta \min \{ \varphi_{1,3}^{h,l_1,l_2,a}(i-(j+2),k), \psi_{1,3}(i-(j+3),k) \}, \quad (17)$$

где $j=4,5,6,7, \dots, (i-l_2)$.

Два последних шага алгоритма (рассматривается случай, для которого $l_2=2$) выполняются по таким схемам: если на $(i-l_2)$ -м шаге формируется исход типа а), то $x_1^{i-1} = x_1^{i-l_2-2}$; если в этом случае возникает исход типа б), то $x_1^{i-1} = x_1^{i-l_2-1}$; если на $(i-l_2)$ -м шаге появляется исход типа б), то $x_1^{i-l_2+1} = x_1^{i-l_2-1}$; если в этом случае формируется исход типа б), то $x_1^i = x_1^{i-l_2}$; если при этом возникает исход типа б), то полуоткрытый интервал $[x_1^{i-l_2}, 1)$ будет разбит на $\varphi_{1,3}^{h,l_1,l_2,a}(i-0,k)$ равных частей.

Заметим, что

$$\begin{aligned} \varphi_{1,3}^{h,l_1,l_2,a}(0,k) &= \varphi_{1,3}^{h,l_1,l_2,a}(1,k) = 1; \\ &\dots \\ \varphi_{1,3}^{h,l_1,l_2,a}(l_2,k) &= 1; \\ \varphi_{1,3}^{h,l_1,l_2,a}(l_2+1,k) &= k+1. \end{aligned} \quad (18)$$

На основании соотношений (14)-(18) устанавливаем такую закономерность:

$$\begin{aligned} \varphi_{1,3}^{h,l_1,l_2,a}(i,k) &= \\ &= \min \{ \varphi_{1,3}^{h,l_1,l_2,a}(i-1,k), \psi_{1,3}(i-k,k) \} + \\ &+ \min \{ \varphi_{1,3}^{h,l_1,l_2,a}(i-3,k), \psi_{1,3}(i-5,k) \} + \\ &+ \min \{ \varphi_{1,3}^{h,l_1,l_2,a}(i-5,k), \psi_{1,3}(i-6,k) \} + \\ &+ \sum_{j=4}^{i-l_2} \min \{ \varphi_{1,3}^{h,l_1,l_2,a}(i-(j+2),k), \\ &\psi_{1,3}(i-(j+3),k) \} + 1. \end{aligned} \quad (19)$$

Поскольку детально было рассмотрено распределение точек экспериментов для всевозможных исхо-

дов типа а) и типа б), то обобщенная логическая схема алгоритма не приводится.

Анализ процедур выбора точек экспериментов позволяет утверждать:

— если на $1, 2, \dots, j$ -м, где $j < l_2 + 1$, шагах алгоритма возникает исход типа б), то точка следующего эксперимента выбирается согласно соотношению:

$$x_1^{j+1} \in (x_1^j, 1); \quad (20)$$

— если $j = (l_2 + 1)$ и на этом шаге снова возникает исход типа б), то происходит уменьшение длины интервала неопределенности относительно точки x с характерным признаком (для нашего примера $x \in [x^2 \dots x^{l_2+1}]$);

— если в процессе поиска на j -м шаге возникает исход типа а), то применяют принцип “повторных сравнений” [4] к каждой точке выбранных ранее экспериментов, расположенной вне границ сформированного интервала неопределенности (таких точек не может быть больше величины l_2);

— если при использовании принципа “повторных сравнений” возникают исходы типа а), то применяют классический алгоритм поиска к полуоткрытому интервалу, расположенному слева от точки повторного эксперимента;

— если при использовании принципа “повторных сравнений” возникают исходы типа б) и справа от точки повторного эксперимента есть другие точки выполненных экспериментов, то к первой из них применяют принцип “повторных сравнений”;

— если при использовании принципа “повторных сравнений” возникают исходы типа б), а справа от точки повторного эксперимента нет других точек выполненных ранее экспериментов, то точка x с характерным признаком будет принадлежать полуоткрытому интервалу неопределенности, расположенному справа от точки повторного эксперимента; этот полуоткрытый интервал за оставшиеся $(i-j-z)$ -шагов алгоритма будет разбит на $\varphi_{1,3}^{h,l_1,l_2,a}(i-j-z,k)$ равных частей, где $z \leq l_2$.

Используя эти правила выделения нового полуоткрытого интервала неопределенности и выбора точки следующего эксперимента, для других значений параметра l_2 получены такие соотношения:

$l_2=3$;

$$\begin{aligned} \varphi_{1,3}^{h,l_1,l_2,a}(i,k) &= \\ &= \min \{ \varphi_{1,3}^{h,l_1,l_2,a}(i-1,k), \psi_{1,3}(i-5,k) \} + \\ &+ \min \{ \varphi_{1,3}^{h,l_1,l_2,a}(i-3,k), \psi_{1,3}(i-6,k) \} + \\ &+ \min \{ \varphi_{1,3}^{h,l_1,l_2,a}(i-5,k), \psi_{1,3}(i-7,k) \} + \\ &+ \min \{ \varphi_{1,3}^{h,l_1,l_2,a}(i-7,k), \psi_{1,3}(i-8,k) \} + \\ &+ \sum_{j=5}^{i-l_2} \min \{ \varphi_{1,3}^{h,l_1,l_2,a}(i-(j+3),k), \\ &\psi_{1,3}(i-(j+4),k) \} + 1. \end{aligned} \quad (21)$$

$l_2=4$;

$$\begin{aligned} \varphi_{1,3}^{h,l_1,l_2,a}(i,k) = & \\ = \min \{ & \varphi_{1,3}^{h,l_1,l_2,a}(i-1,k), \psi_{1,3}(i-6,k) \} + \\ + \min \{ & \varphi_{1,3}^{h,l_1,l_2,a}(i-3,k), \psi_{1,3}(i-7,k) \} + \\ + \min \{ & \varphi_{1,3}^{h,l_1,l_2,a}(i-5,k), \psi_{1,3}(i-8,k) \} + \\ + \min \{ & \varphi_{1,3}^{h,l_1,l_2,a}(i-7,k), \psi_{1,3}(i-9,k) \} + \\ + \min \{ & \varphi_{1,3}^{h,l_1,l_2,a}(i-9,k), \psi_{1,3}(i-10,k) \} + \\ + \sum_{j=6}^{i-l_2} \min \{ & \varphi_{1,3}^{h,l_1,l_2,a}(i-(j+4),k), \\ \psi_{1,3}(i-(j+5),k) & \} + 1. \end{aligned} \quad (22)$$

$l_2=5$;

$$\begin{aligned} \varphi_{1,3}^{h,l_1,l_2,a}(i,k) = & \\ = \min \{ & \varphi_{1,3}^{h,l_1,l_2,a}(i-1,k), \psi_{1,3}(i-7,k) \} + \\ + \min \{ & \varphi_{1,3}^{h,l_1,l_2,a}(i-3,k), \psi_{1,3}(i-8,k) \} + \\ + \min \{ & \varphi_{1,3}^{h,l_1,l_2,a}(i-5,k), \psi_{1,3}(i-9,k) \} + \\ + \min \{ & \varphi_{1,3}^{h,l_1,l_2,a}(i-7,k), \psi_{1,3}(i-10,k) \} + \\ + \min \{ & \varphi_{1,3}^{h,l_1,l_2,a}(i-9,k), \psi_{1,3}(i-11,k) \} + \\ + \min \{ & \varphi_{1,3}^{h,l_1,l_2,a}(i-11,k), \psi_{1,3}(i-12,k) \} + \\ + \sum_{j=7}^{i-l_2} \min \{ & \varphi_{1,3}^{h,l_1,l_2,a}(i-(j+5),k), \\ \psi_{1,3}(i-(j+6),k) & \} + 1. \end{aligned} \quad (23)$$

Анализ соотношений (19), (21)-(23) показывает, что перед символом $\sum$ они дополнительно содержат (l_2+1) слагаемых; каждое из этих слагаемых содержит два элемента; аргумент первого элемента первого слагаемого равен $(i-1, k)$, аргумент второго элемента первого слагаемого равен $(i-(l_2+2), k)$; аргумент первого элемента второго слагаемого равен $(i-3, k)$; аргумент второго элемента второго слагаемого равен $(i-(l_2+3), k)$ и т.д., аргумент первого элемента (l_2+1) -го слагаемого равен $(i-(2l_2+1), k)$; аргумент второго элемента (l_2+1) -го слагаемого равен $(i-(2l_2+2), k)$; наименьшее значение индекса j равно $j=l_2+2$; значение аргумента первого элемента первого слагаемого, входящего под знак $\sum$, равно $(i-(j+l_2), k)$, аргумент второго элемента первого слагаемого равен $(i-(j+l_2+1), k)$.

С учетом сделанных обобщений получаем соотношения для преобразованного значения параметра l_2 :

$$\begin{aligned} \varphi_{1,3}^{h,l_1,l_2,a}(i,k) = & \\ = \sum_{\beta=0}^{l_2} \min \{ & \varphi_{1,3}^{h,l_1,l_2,a}(i-2\cdot\beta-1,k), \\ \psi_{1,3}(i-(l_2+2+\beta),k) & \} + \\ + \sum_{j=l_2+2}^{i-l_2} \min \{ & \varphi_{1,3}^{h,l_1,l_2,a}(i-(j+k),k), \\ \psi_{1,3}(i-(j+l_2+1),k) & \} + 1. \end{aligned} \quad (24)$$

Поиск точки x с характерным признаком осуществляется по описанной выше схеме, начиная с первого и кончая шагом алгоритма, для которого выполняется соотношение: $(i-j)=l_2$.

Как только будет совершен последний такой шаг, то независимо от исхода следует применить принцип "повторных сравнений". Запишем очевидные соотношения как:

$$\begin{aligned} \varphi_{1,3}^{h,l_1,l_2,a}(0,k) &= \varphi_{1,3}^{h,l_1,l_2,a}(1,k) = \\ &= \varphi_{1,3}^{h,l_1,l_2,a}(l_2,k) = 1; \\ \varphi_{1,3}^{h,l_1,l_2,a}(l_2+1,k) &= k+1. \end{aligned} \quad (25)$$

Описанные стратегии поиска (закономерности распределения точек экспериментов), правила формирования нового интервала неопределённости и логические схемы алгоритмов поиска позволяют методом индукции построить алгоритм для любых его параметров и любых параметров $A_{1,3}$ -последовательности, и тем самым разработать оригинальные методы защиты информации.

Литература: 1 Алипов Н.В. Разработка теории и методов решения задач помехоустойчивого алгоритма поиска и преобразования информации//Автореферат дис. на соискание учёной степени доктора технических наук. Харьков:ХИРЭ,1986. 50с. 2 Алипов Н. В., Алипов И.Н., Буллах Е.В., Охалник А.А., Ребезюк Л.Н. Датчики виртуальной помехи, используемые для организации функционирования дискретных автоматов в системах защиты информации // Радиотехника. 1999. Вып. 111. С.33-39. 3. Альсведе Р., Вегенер М. Задачи поиска. М: Мир, 1982. 365с. 4. Алипов Н.В. Принцип "пересечения" и его применение при алгоритмическом синтезе преобразователей информации. К.: Наук. думка. 1980. С.10-13.

Поступила в редколлегию 18.04.2000

Рецензент: д-р техн. наук, проф. Руденко О.Г.

Алипов Николай Васильевич, д-р техн. наук, профессор кафедры проектирования и эксплуатации электронных аппаратов ХТУРЭ. Научные интересы: защита информации, алгоритмизация задач автоматизированного проектирования электронных вычислительных средств. Адрес: Украина, 61189, Харьков, ул. Иртышская, 8, тел. 40-94-94.

Алипов Илья Николаевич, канд. техн. наук. Научные интересы: защита информации. Адрес: Украина, 61189, Харьков, ул. Иртышская, 8, тел. 40-94-94.

Беляев Сергей Александрович, студент группы САПР-95-1 ХТУРЭ. Научные интересы: защита информации. Адрес: 61007, Харьков, ул.Салтовское шоссе, 256, кв. 261, тел. 10-17-51.

Ребезюк Леонид Николаевич, канд. техн. наук, доцент кафедры проектирования и эксплуатации электронных аппаратов ХТУРЭ. Научные интересы: защита информации, алгоритмизация задач автоматизированного проектирования электронных вычислительных средств. Адрес: Украина, 61136, Харьков, ул. Ком. Уборевича, 40-б, кв. 17, тел. 69-79-38.