УДК 681.3+681.5:007

Н.В. АЛИПОВ, А.А. ОХАПКИН, Л.Н. РЕБЕЗЮК

ЗАЩИТА ИНФОРМАЦИИ В ДИСКРЕТНОМ КАНАЛЕ НА ОСНОВЕ УСТОЙЧИВЫХ К ПЕРИОДИЧЕСКИМ ПОМЕХАМ АЛГОРИТМОВ ПОИСКА ТОЧКИ С ХАРАКТЕРНЫМ ПРИЗНАКОМ

В работе синтезируются алгоритмы поиска точки с характерным признаком на отрезке [0, 1] в условиях воздействия на входе дискретного автомата периодических помех.

Для того чтобы синтезировать алгоритм поиска, задающий функционирование дискретного автомата в условиях воздействия периодических помех, необходимо задаться параметрами алгоритма (количеством его шагов и количеством точек эксперимента k), а затем построить решающую функцию (правила выделения нового интервала неопределенности относительно точки с характерным признаком) и определить стратегию поиска (закономерности распределения k точек эксперимента во вновь выделенном интервале неопределенности относительно x) [3].

Периодическая помеха будет описываться максимально возможной амплитудой ah (h — дискретность преобразования) и длительностью импульса λ. Оценкой алгоритма поиска является функция $\Psi_{\text{п}}^{a,\lambda}(i,k)$. В дальнейшем будем рассматривать случай, когда $\lambda = \Delta t$, где Δt — длительность шага алгоритма.

Воспользуемся основными понятиями и определениями, изложенными в работе [3]. Для подавления периодической помехи будем исходить из того, что если в момент времени t_1 найдено значение смеси сигнала и помехи $x(t_1)$, а затем определено новое значение в момент времени $(t_1 + \Delta t)$, то координаты искомой точки определяются соотношением

$$x = \left[x(t_1) + x(t_1 + \Delta t)\right]/2, \qquad (1)$$

где $x(t_1) = x + \xi(t_1)$; $x(t_1 + \Delta t) = x + \xi(t_1 + \Delta t)$, $\xi(t_1)$ – помеха, накладываемая на сигнал в момент времени t_1 и $|\xi(t_1)| = |\xi(t_1 + \Delta t)|$.

Поскольку в процессе поиска выделяется минимальное $x_{\min} = x - ah$ и максимальное $x_{\max} = x + ah$ значение смеси сигнала и помехи, то исходным интервалом неопределенности относительно $x_{\min}$ и $x_{\max}$ будет интервал $[-a, 1+a]$.

Пусть некоторым образом выбраны в интервале неопределенности $[-a, 1+a]$ относительно $x_{\min}$ и $x_{\max}$ k точек эксперимента. Тогда может возникнуть один из исходов $x(t_1) \in \left[x_{\text{q}}^1, x_{q+1}^1\right)$, $q = \overline{0,k}$.

На основании принципа "пересечения" [3] устанавливаем

$$x_{\min}, x_{\max} \in \left[x_q^{1,1}, x_{q+1}^{1,2}\right), \tag{2}$$

где

$$x_q^{1,1} = \begin{cases} x_q^1 - 2ah, \text{если } x_q^1 - 2ah \geq -a; \\ -a \text{ в противном случае}, \end{cases}$$

$$x_{q+1}^{1,1} = \begin{cases} x_{q+1}^1 + 2ah, \text{ если } x_{q+1}^1 + 2ah \leq 1 + a; \\ 1 + a \text{ в противном случае}. \end{cases}$$

Пусть на $(j\text{-}1)$-м шаге установлено, что $(x + \xi(t_1 + (j-2)\Delta t) \in \left[x_q^{j-1}, x_{q+1}^{j-1}\right)$. При выполнении j-го шага точки $x_{q_1}^j$ выбраны так, что они принадлежат интервалу $\left(x_q^{j-1}, x_{q+1}^{j-1}\right)$, $q = \overline{0,k}$, и выделяется интервал неопределенности $\left(x_{\beta}^{\text{j}}, x_{\beta+1}^j\right)$. Тогда относительно $x_{\min}$, $x_{\max}$ формируется интервал неопределенности:

$$x_{\min}, x_{\max} \in \left[x_{\beta}^{\text{j},1}, x_{\beta+1}^{j,2}\right), \tag{3}$$

где

$$x_{\beta}^{j,1} = \begin{cases} x_{\beta}^j - 2ah, \text{ если } x_{\beta}^j - 2ah \geq x_q^{j-1,1}; \\ x_q^{j-1,1} \text{ в противном случае}, \end{cases}$$

$$x_{\beta+1}^{j,2} = \begin{cases} x_{\beta+1}^{j} + 2ah, \text{ если } x_{\beta+1}^{j,2} + 2ah \le x_{\beta+1}^{j-1,2}; \\ x_{\beta+1}^{j-1,2} \text{ в противном случае}. \end{cases}$$

На некоторых шагах при поиске $x_{\min}$ и $x_{\max}$ применяют смешанную стратегию [3].

Пусть на j-м шаге γ_1 точек эксперимента размещена в левом расширении $\left(x_q^{j-1,1}, x_q^{j-1}\right)$, γ_2 точек — в основном интервале $\left(x_q^{j-1}, x_{q+1}^{j-1}\right)$, а оставшиеся – в правом расширении $\left[x_{q+1}^{j-1}, x_{q+1}^{j-1,2}\right)$. В этой ситуации может возникнуть один из исходов:

$б_1)\ x\left(t_1 + j\Delta t\right) \in \left[x_{q_1}^{j}, x_{q_1+1}^{j}\right),\ q_1 = \overline{0, \gamma_1};$

$б_2)\ x\left(t_1 + j\Delta t\right) \in \left[x_{q_2}^{j}, x_{q_2+1}^{j}\right),\ q_2 = \overline{\gamma_1 + 1, \gamma_1 + \gamma_2};$

$б_3)\ x\left(t_1 + j\Delta t\right) \in \left[x_{q_3}^{j}, x_{q_3+1}^{j}\right),\ q_3 = \overline{\gamma_1 + \gamma_2 + 1, k}.$

Если возник исход $б_1$, то для него характерно проявление помехи отрицательной полярности. В этом случае относительно $x_{\min}, x_{\max}$ выделяется полуоткрытый интервал:

$$x_{\min} \in \left[x_{q_1}^{j}, x_{q_1+1}^{j}\right);\ x_{\max} \in \left[x_{q_1+1}^{j}, x_{q_1+1}^{j,2}\right), \tag{4}$$

где $x_{q_1+1}^{j,2} = x_{q_1+1}^{j} + 2ah.$

Для исхода $б_2$ интервал неопределенности формируется согласно соотношению (3).

Для исхода $б_3$ характерно проявление помехи положительной полярности и в этом случае выделяется полуоткрытый интервал:

$$x_{\min} \in \left[x_{q_3}^{j,1}, x_{q_3}^{j}\right);\ x_{\max} \in \left[x_{q_3}^{j}, x_{q_3+1}^{j}\right), \tag{5}$$

где $x_{q_3}^{j,1} = x_{q_3}^{j} - 2ah.$

Полученные соотношения (1)—(5) позволяют для любого исхода сформировать новые интервалы неопределенности относительно $x_{\min}, x_{\max}$; тем самым они задают решающую функцию алгоритма.

Выявим закономерности распределения точек эксперимента на $(j+1)$-м шаге алгоритма в полученном открытом интервале $\left[x_{\rho_1}^{j,1}, x_{\rho_1+1}^{j,2}\right)$.

Если точки эксперимента на $(j+1)$-м шаге размещаются в интервале $\left[x_{\rho_1}^{j}, x_{\rho_1+1}^{j}\right)$, то такая стратегия называется оптимистической [4]. Если же точки эксперимента на $(j+1)$-м шаге размещаются в интервале $\left[x_{\rho_1}^{j,1}, x_{\rho_1+1}^{j,2}\right)$, то такая стратегия называется смешанной [4].

Нетрудно заметить, что если $i=1$, то $\Psi_{\text{п}}^{a,1}(1,k)=1$ (в условиях помех интервал неопределенности нельзя уменьшить). Если же $i=2$, то применяется принцип "повторных сравнений" [3], исходный интервал $(-a,\ 1+a)$ разбивается равномерно, поэтому

$$\Psi_{\text{п}}^{a,2}(2,k)=k+1. \tag{6}$$

На размещение точек эксперимента существенное влияние оказывает амплитуда помехи. Можно показать, что если

$$2ah \geq h(k+1)^{]i/2[}, \tag{7}$$

то оптимальным будет алгоритм:

$(j+1)$-й шаг. Равномерно разместить в $\left[x_q^j, x_{q+1}^j\right)$ точки эксперимента $x_{q_1}^{j+1}=q_1(x_{q+1}^j-x_q^j)\big/(k+1)$, $q_1=\overline{1,k}$ и выделить новый полуоткрытый интервал $\left[x_{q_2}^{j+1}, x_{q_2+1}^{j+1}\right)$, $q_2=\overline{0,k}$;

$(j+2)$-й шаг. Равномерно разместить в $\left[x_q^j, x_{q+1}^j\right)$ точки эксперимента, выделить новый полуоткрытый интервал неопределенности $\left[x_\beta^{j+2}, x_{\beta+1}^{j+2}\right)$, $\beta=\overline{0,k}$.

Если $q_2=\beta$, то следующие два шага алгоритма совершаются в $\left[x_{q_2}^{j+1}, x_{q_2+1}^{j+1}\right)$ аналогично $(j+1)$-му и $(j+2)$-му шагам алгоритма.

Если $q_2 \neq \beta$, то $(j+3)$-й и $(j+4)$-й шаги алгоритма выполняются следующим образом:

$(j+3)$-й шаг. Точки эксперимента разместить равномерно в полуоткрытом интервале $\left[x_{q_2}^{j+1}, x_{q_2+1}^{j+1}\right)$, выделить новый полуоткрытый интервал $\left[x_{q_3}^{j+3}, x_{q_3+1}^{j+3}\right)$, $q_3 = \overline{0,k}$;

$(j+4)$-й шаг. Равномерно разместить в $\left[x_{\beta}^{j+2}, x_{\beta+1}^{j+2}\right)$ точки эксперимента, выделить $\left[x_{\beta_1}^{j+4}, x_{\beta_1+1}^{j+4}\right)$, $\beta_1 = \overline{0,k}$.

Следующие два шага алгоритма совершить аналогичным образом, как совершались $(j+3)$-й и $(j+4)$-й шаги алгоритма. Данный алгоритм назовем **$A_п$**-алгоритмом.

Следует заметить, что если $x_{q_2}^{j+1} < x_{\beta+1}^{j+2}$, то на $(j+1)$-м шаге действует помеха отрицательной полярности, а на $(j+2)$-м — положительной полярности. Если $x_{q_2}^{j+1} > x_{\beta+1}^{j+2}$, то на указанных интервалах полярность помехи противоположна. В таких случаях на $(j+3)$-м шаге точки эксперимента равномерно размещаются в интервале $\left[x_{q_2}^{j+1}, x_{q_2+1}^{j+1}\right)$, а на $(j+4)$-м — в интервале $\left[x_{\beta}^{j+2}, x_{\beta+1}^{j+2}\right)$. Каждый из указанных интервалов будет разбит на m_1 и m_2 равных частей:

$$m_1 = \begin{cases} (k+1)^{\frac{i-j}{2}}, \text{ если } \textit{(i-j)}\text{- четное число;} \\ (k+1)^{\left]\frac{i-j}{2}\right[+1}, \text{в противном случае,} \end{cases}$$
$$m_2 = (k+1)^{\left]\frac{i-j}{2}\right[}, \qquad (8)$$

где $\left]\frac{i-j}{2}\right[$ — целая часть от деления $\frac{i-j}{2}$.

Когда соотношение (7) не выполняется, то принцип "повторных сравнений" применяется не с первого шага. Шаг алгоритма, на котором применяется принцип "повторных сравнений", определяется следующим утверждением:

S1. Если $\left(x+\xi\left(t_j\right)\right) \in \left[x_q^j, x_{q+1}^j\right)$ и имеют место соотношения:

$$h(1+\gamma_1)(k+1)^{\left\lceil \frac{i-j-(2n+1)}{2} \right\rceil} > (x_q^j - x_{q-1}^{j,1}),$$ а

$$h(k_1+1)(k+1)^{\left\lceil \frac{i-j-(2n+1)}{2} \right\rceil} > (x_{q+1}^{j,2} - x_{q+1}^j),$$

где

$$\gamma_1 = \begin{cases} 1, \text{ если } (i-j) \text{ - нечетное число;} \\ \le k \text{ в противном случае,} \end{cases}$$

$$k_1 = \begin{cases} 1, \text{ если } (i-j) \text{ - нечетное число;} \\ \le k \text{ в противном случае,} \end{cases}$$

то при условии, что $n > 1,\ (\gamma_1 + k_1) < k$, имеет место оптимистическая стратегия:

$$x_{q_2}^{j+1} \in \left(x_q^j, x_{q+1}^j\right),\quad q_2 = \overline{1,k};$$

при условии, что $n = 0,\ (\gamma_1 + k_1) \le k$, применяется смешанная стратегия (γ_1 точек эксперимента согласно схеме классического алгоритма поиска размещаются в полуоткрытом интервале $(x_q^{j,1}, x_q^j],\ k_1$ точек эксперимента – в полуоткрытом интервале $[x_{q+1}^j, x_{q+1}^{j,2})$, а остальные $(k-\gamma_1-k_1)$ точек – в интервале (x_q^j, x_{q+1}^j));

в случаях, когда $n > 0,\ (\gamma_1 + k_1) > k$ или $k_1 = k,\ \gamma_1 > k$, применяется смешанная стратегия, для которой характерно такое распределение точек эксперимента:

$$x_1^{j+1} = x_q^j,\ x_k^{j+1} = x_{q+1}^j,$$
$$x_{q_3}^{j+1} \in (x_q^j, x_{q+1}^j),\quad q_3 = \overline{2,k-1};$$

при условии, что $n > 1,\ \gamma_1 = 0,\ k_1 > k$, применяется смешанная стратегия такого вида:

$$x_k^{j+1} = x_{q+1}^j,\ x_{q_4}^{j+1} \in (x_q^j, x_{q+1}^j),\quad q_4 = \overline{1, k-1};$$

при истинности соотношений: $n > 1,\ \gamma_1 > k,\ k_1 \le k$ используется смешанная стратегия такого вида:

$$x_1^{j+1} = x_q^j,\ x_{q_5}^{j+1} \in (x_q^j, x_{q+1}^j),\quad q_5 = \overline{2, k}.$$

Полученные соотношения для решающей функции и стратегии поиска позволяют синтезировать помехоустойчивый алгоритм поиска точки с характерным признаком по такой схеме:

1. Если соотношение (7) выполняется, то применить $\mathbf{A_п}$-алгоритм и перейти к п.8, иначе – к п. 2.

2. Построить $(i-1)$-й шаговый алгоритм поиска в условиях воздействия периодических помех. Индексу z' присвоить значение, равное единице.

3. Сформировать возможный исход. Если все исходы сформированы, то перейти к п.8, в противном случае — к п.4.

4. Используя утверждение S1, распределить точки эксперимента, затем, на основании соотношений (1)—(6), выделить интервал неопределенности относительно $x = x + \xi(\Delta t)$.

5. Положить $z' = z'+1$ и, если $z' \ge 1$, то перейти к п.6, в противном случае — к п.7.

6. Сформировать возможный исход на z'-м шаге алгоритма. Если все исходы сформированы — перейти к п.7, иначе перейти к п.4.

7. Положить $z' = z'-1$ и $z' = 2$ — перейти к п.3, в противном случае перейти к п.6.

8. Алгоритм построен.

По этой схеме можно построить для любых a и k помехоустойчивый к периодическим помехам алгоритм поиска точки с характерным признаком на отрезке единичной длины и, тем самым, определить функционирование дискретного автомата системы защиты информации.

Список литературы: 1. *Ecker A.* Abstrakte kryptographische Maschinen // Angew. Informatik. 1975. Bd. 17, Nr 5, P. 201-205. 2. *Алипов И.Н., Ребезюк Л.Н.* Постановка задачи синтеза новых методов защиты информации // Радиотехника. Харьков, ХТУРЭ, 1997. Вып. 103. С. 60-64. 3. *Алипов Н.В.*

Разработка теории и методов решения задач помехоустойчивого поиска и преобразования информации. Автореферат диссертации на соискание ученой степени доктора технических наук. Харьков, ХИРЭ, 1986. 48 с.
4. *Алипов И.Н.* Помехоустойчивые к А1-последовательности алгоритмы поиска точки экстремума унимодальной функции // АСУ и приборы автоматики. Харьков, ХТУРЭ. 1997. Вып. 104. С. 69-75.

Поступила в редколлегию 30.11.98

Алипов Николай Васильевич, д-р техн. наук, профессор кафедры конструирования электронно-вычислительных машин ХТУРЭ. Научные интересы: защита информации, алгоритмизация задач автоматизированного проектирования электронных вычислительных средств. Адрес: Украина, 310189, Харьков, ул. Иртышская, 8, тел. 40-94-25.

Охапкин Александр Александрович, аспирант кафедры конструирования электронно-вычислительных машин ХТУРЭ. Научные интересы: защита информации. Адрес: Украина, 310007, Харьков, ул. Бекетова 19/17, кв. 21, тел. 40-94-25.

Ребезюк Леонид Николаевич, канд. техн. наук, доцент кафедры конструирования электронно-вычислительных машин ХТУРЭ. Научные интересы: защита информации, системы автоматизированного проектирования. Адрес: Украина, 310136, Харьков, ул. Ком. Уборевича, 40-б, кв. 17, тел. 69-79-38.

УДК 621.396.96

Н.И. МАТЮХИН

ДВУСТОРОННЕЕ УПРАВЛЕНИЕ СОСТОЯНИЕМ МНОГОФУНКЦИОНАЛЬНОЙ ЛОКАЦИОННО-ГОЛОГРАФИЧЕСКОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ В ФОРМЕ ДИФФЕРЕНЦИАЛЬНОЙ ИГРЫ "НАБЛЮДЕНИЕ—ПРОТИВОДЕЙСТВИЕ"

---

1. Постановка задачи

Современные радиолокационные системы представляют собой сложные динамические системы с ограниченным ресурсом и с высокой стоимостью. Под ресурсом системы понимается резерв аппаратуры, энергии и времени, необходимый для наблюдения потока целей с определенным качеством в условиях противодей-