можно использовать ширину термопрофиля между точками, в которых происходит изменение знака производной по координате (т. С1, С2 на рис.3), или "эффективную" ширину термопрофиля в виде расстояния между точками, в которых $T_{эф}=T_{мах}$ / 1,41.

В дальнейшем предполагается применение новых методов решения ОЗ теплопроводности (например, численно-аналитических), которые позволяют осуществить контроль трубопровода в реальном масштабе времени, т.е. непосредственно в процессе измерений температурного распределения на поверхности грунта.

6. Выводы

1. Создана теплофизическая модель трубопровода, пролегающего в грунте, а также компьютерная программа, позволяющая моделировать тепловые процессы в системе "трубопровод-грунт-воздух".

2. Экспериментальные исследования показали достаточную адекватность построенной модели.

3.Построены справочные диаграммы, позволяющие на практике по температурному распределению на поверхности грунта определять параметры трубопровода.

Литература: 1.*АлексеевА.А.* Упредить возможность аварий // Экология и промышленность России. 1996. С.4-5. 2.*Троицкий В.А.* Опыт применения компьютерной системы P-scan для оценки качества металла оборудования тепловых и атомных электростанций // Друга Українська науково-технічна конференція "Неруйнівний контроль та технічна діагностика", Дніпропетровськ, 1997. С.154. 3.*Самарский А.А., Гурин А.В.* Численные методы. М.: Наука, 1989. 259с. 4. *Миснар А.* Теплопроводность твердых тел, жидкостей, газов и их композиций. М.: Мир, 1988. 464 с. 5.*ГригорьевИ.С., Мелихов Е.З.* Физические величины. Справочник. М.: Энергоатомиздат, 1991. 1195 с.

Поступила в редколлегию 08.06.01

Рецензент: д-р физ.-мат. наук, проф. Исаев А.А.

Кухарев Юрий Александрович, аспирант кафедры физики ХНУРЭ. Научные интересы: тепловой неразрушающий контроль в энергетике и трубопроводном транспорте. Увлечения и хобби: программирование на Visual C. Адрес: Украина, 61000, Харьков, пер.17 Партсъезда, 6, кв.84, тел.40-93-45.

УДК 681.3+681.5:007

ПРИМЕРЫ ПОСТРОЕНИЯ ПОМЕХОУСТОЙЧИВЫХ К СИММЕТРИЧНЫМ НЕРЕГУЛЯРНЫМ ВИРТУАЛЬНЫМ ПОСЛЕДОВАТЕЛЬНОСТЯМ АЛГОРИТМОВ ПОИСКА ТОЧКИ С ХАРАКТЕРНЫМ ПРИЗНАКОМ

АЛИПОВ Н.В., АЛИПОВ И.Н., ЛИТВИНОВА Е.И, РЕБЕЗЮК Л.Н.

Строятся алгоритмы поиска точки с характерным признаком, помехоустойчивые к симметричным нерегулярным виртуальным последовательностям. Эти алгоритмы задают функционирование дискретных автоматов с псевдослучайными переходами систем защиты информации.

В работе [1] описана стратегия поиска, правила формирования нового интервала неопределенности и логическая схема помехоустойчивых к симметричным нерегулярным виртуальным последовательностям алгоритмов поиска точки на отрезке единичной длины.

В предлагаемом исследовании разрабатываются примеры таких алгоритмов, синтезированных для конкретных их параметров и параметров виртуальной последовательности.

Первоначально рассмотрим случай, для которого примечательно то, что $l_1=1$, $l_2=2$, $H=3$, $k=1$, $a=\infty$, построение алгоритмов поиска осуществим методом индукции по i.

На основании соотношения (2) [1] устанавливаем, что для указанных параметров алгоритма уменьшение исходного интервала неопределенности относительно точки с характерным признаком первоначально произойдет для $i=5$. В этом случае, как известно [1], используется принцип "повторных сравнений" по такой схеме:

1-й шаг: выполнить эксперимент в точке $x_1^1=h$.

2-й шаг: повторить эксперимент.

3-й шаг: повторить эксперимент.

4-й шаг: если по итогам выполнения третьего эксперимента алгоритма возникает исход типа $а_{11}$) [1], то $x\in\left[0,x_1^1\right)$; $l\left(\left[0,x_1^1\right)\right)=h\varphi_{2,3}^{3,1,2,\infty}(5{-}3,1)=h$;

если же по итогам выполнения третьего эксперимента алгоритма возникает исход типа $б_{22}$) [1], то

$x\in\left[x_1^1,1\right)$; $l\left(\left[x_1^1,1\right)\right)=h\varphi_{2,3}^{3,1,2,\infty}(5{-}3,1)=h$;

если по итогам выполнения третьего эксперимента алгоритма возникает исход типа $а_{21}$) [1], то это свидетельствует о проявлении виртуальной последовательности на втором шаге алгоритма, на этом основании устанавливаем: $x\in\left[0,x_1^1\right)$; четвертый и пятый шаги являются первым и вторым шагами классического алгоритма поиска:

$$l\left(\left[0,x_1^1\right)\right)=h\psi_{2,3}(5{-}3,1)=4h\ .$$

Если же по итогам выполнения третьего эксперимента алгоритма возникает исход типа $б_{12}$) [1], то это свидетельствует о действии помехи на втором

шаге; на этом основании заключаем: $x \in \left[x_1^1, 1\right)$; четвёртый и пятый шаги являются первым и вторым шагами классического алгоритма поиска:

$$l\left(\left[x_1^1, 1\right)\right) = h\psi_{2,3}(5-3,1) = 4h ;$$

для всех других исходов повторяем эксперимент.

5-й шаг: если по итогам выполнения четвертого шага алгоритма формируется один из исходов типа a_{121}), a_{221}), $б_{111}$) [1], то устанавливаем:

$x \in \left[0, x_1^1\right)$; пятый шаг есть первый шаг классического алгоритма поиска:

$$l\left(\left[0, x_1^1\right)\right) = 2h ;$$

если по итогам выполнения четвертого шага алгоритма появляется один из исходов типа a_{222}), $б_{112}$), $б_{212}$) [1], то устанавливаем:

$x \in \left[x_1^1, 1\right)$; пятый шаг есть первый шаг одношагового классического алгоритма поиска:

$$l\left(\left[x_1^1, 1\right)\right) = 2h ;$$

для всех других исходов повторяем эксперимент.

Если по итогам выполнения пятого шага алгоритма формируется один из исходов типа a_{1221}), $б_{2111}$) [1], то $x \in \left[0, x_1^1\right)$, $l\left(\left[0, x_1^1\right)\right) = h$;

если же по итогам выполнения пятого шага алгоритма формируется один из исходов типа a_{1222}), $б_{2112}$) [1], то $x \in \left[x_1^1, 1\right)$, $l\left(\left[x_1^1, 1\right)\right) = h$.

Из приведенной схемы алгоритма поиска следует, что в самом наихудшем случае первоначальный интервал неопределенности будет разбит на две равные части. На этом основании подтверждаем истинность выражения

$$\varphi_{2,3}^{3,1,2,\infty}(5,1) = 2 . \qquad (1)$$

Пусть $i = 6$ и по итогам выполнения первых трёх шагов сформирован исход типа a_{11}) либо типа $б_{22}$) [1]. Тогда это означает, что на следующем, четвёртом шаге в обязательном порядке будет действовать очередной выброс виртуальной последовательности. Применить на четвёртом шаге алгоритма в полном объёме смешанную стратегию не удается. По этой причине используем её на четвертом и пятом шагах алгоритма:

четвёртый шаг: $x_1^4 = x_1^1$;

пятый шаг: если по итогам выполнения четвертого шага алгоритма формируется один из исходов:

a_{111}) $x + \zeta(t) < x_1^1$; a_{112}) $x + \zeta(t) > x_1^1$;

$б_{221}$) $x + \zeta(t) < x_1^1$; $б_{222}$) $x + \zeta(t) > x_1^1$,

то для исхода типа a_{112}) характерно действие на четвёртом шаге выброса положительной полярности, для исхода типа $б_{221}$) — действие выброса отрицательной полярности (для этих исходов пропускаем пятый шаг алгоритма);

для исхода типа a_{111}) характерно действие выброса отрицательной полярности, для исхода типа $б_{222}$) — действие выброса положительной полярности (пятый шаг и в этих случаях пропускается).

Шестой шаг: для исходов типа a_{111}), a_{112}) точку шестого эксперимента выбираем согласно соотношению $x_1^6 = h$;

для исходов типа $б_{221}$), $б_{222}$) точку шестого эксперимента выбираем на основании выражения $x_1^6 = x_1^1 + h$.

Поскольку на шестом шаге алгоритма действие виртуальной последовательности не будет наблюдаться, то классический алгоритм разбивает каждый из полуоткрытых интервалов $\left[0, x_1^1\right)$, $\left[x_1^1, 1\right)$ на две равные части, следовательно, $\psi_{2,3}^{**}(5-3,1) = 2$.

Если бы на четвёртом и пятом шагах алгоритма поиск точки с характерным признаком не продолжался по такой схеме, то, как известно, для исхода типа a_{11}) $x \in \left[0, x_1^1\right)$, для исхода типа $б_{22}$) $x \in \left[x_1^1, 1\right)$, и каждый из этих полуоткрытых интервалов был бы разбит на $\varphi_{2,3}^{3,1,2,\infty}(6-3,1)$ равных частей.

В свою очередь, если бы в результате поиска был сформирован один из исходов типа a_{1222}) [1] либо типа $б_{2111}$) [1], то в первом случае полуоткрытый интервал $\left[x_1^1, 1\right)$, а во втором — $\left[0, x_1^1\right)$ были бы разбиты на $\psi'_{2,3}(6-5,1)$ равные части. Для этой функции справедливо равенство $\psi'_{2,3}(6-5,1) = 1$.

Поэтому для функции $\varphi_{2,3}^{3,1,2,\infty}(6,1)$ справедливо соотношение

$$\varphi_{2,3}^{3,1,2,\infty}(6,1) = 2\min\left\{\psi'_{2,3}(6-5,1), \max\left\{\psi_{2,3}^{**}(6-3,1), \varphi_{2,3}^{3,1,2,\infty}(6-3,1)\right\}\right\} = 2. \qquad (2)$$

Показано, что для $i = 7$ справедливо равенство $\psi_{2,3}^{3,1,2,\infty}(7,1) = 2$.

Для $i = 8$ будут иметь место такие выражения:

$$\psi'_{2,3}(8-5,1) = 2 ; \quad \psi_{2,3}^{**}(8,1) = 4 ; \quad \varphi_{2,3}^{3,1,2,\infty}(8-3,1) = 2 ;$$

$$\varphi_{2,3}^{3,1,2,\infty}(8,1) = \min 2\left\{\psi'_{2,3}(8-5,1), \max\left\{\psi_{2,3}^{**}(8-3,1), \varphi_{2,3}^{3,1,2,\infty}(8-3,1)\right\}\right\} = 4.$$

Для $i = 9$ соответственно будем иметь:

$$\psi'_{2,3}(9-5,1) = 4 ; \quad \varphi_{2,3}^{3,1,2,\infty}(9-3,1) = 2 ; \psi_{2,3}^{**}(9-3,1) = 4 ;$$

$$\varphi_{2,3}^{3,1,2,\infty}(9,1) = 8 .$$

Для $i = 10$ справедливы такие соотношения:

$$\psi'_{2,3}(10-5,1) = 8 ; \quad \psi_{2,3}^{**}(10-3,1) = 8 ;$$

$$\varphi_{2,3}^{3,1,2,\infty}(10-3,1) = 2 ; \varphi_{2,3}^{3,1,2,\infty}(10,1) = 16 .$$

Для других значений параметра i будем иметь соответственно такие выражения:

$i=11$

$$\psi'_{2,3}(11-5,1)=8;\quad \psi^{**}_{2,3}(11-3,1)=16;$$
$$\varphi^{3,1,2,\infty}_{2,3}(11-3,1)=4;\ \varphi^{3,1,2,\infty}_{2,3}(11,1)=16;$$

$i=12$

$$\psi'_{2,3}(12-5,1)=8;\quad \psi^{**}_{2,3}(12-3,1)=32;$$
$$\varphi^{3,1,2,\infty}_{2,3}(12-3,1)=8;\ \varphi^{3,1,2,\infty}_{2,3}(12,1)=16;$$

$i=13$

$$\psi'_{2,3}(13-5,1)=16;\quad \psi^{**}_{2,3}(13-3,1)=32;$$
$$\varphi^{3,1,2,\infty}_{2,3}(13-3,1)=16;\ \varphi^{3,1,2,\infty}_{2,3}(13,1)=32.$$

Значения функции $\varphi^{3,1,2,\infty}_{2,3}(i,1)$ сведены в таблицу.

i	1	2	3	4	5	6	7	8	9	10	11	12	13
$\varphi^{3,1,2,\infty}_{2,3}(i,1)$	1	1	1	1	2	2	2	4	8	16	16	16	32

Для произвольного i соотношение (2) запишется в таком виде:

$$\varphi^{3,1,2,\infty}_{2,3}(i,1)=2\min\left\{\psi'_{2,3}(i-5,1),\max\left\{\psi^{**}_{2,3}(i-3,1),\ \varphi^{3,1,2,\infty}_{2,3}(i-3,1)\right\}\right\}. \qquad (3)$$

В соотношении (3) из трех его членов известным является последний (для предыдущих значений i значение $\varphi^{3,1,2,\infty}_{2,3}(i-3,1)$ найдено). Чтобы найти значение первого члена этого соотношения, необходимо исходить из таких соображений: виртуальная последовательность не наблюдалась на третьем, четвёртом и пятом шагах алгоритма: для $H=3$ эта последовательность в самом неблагоприятном случае будет проявляться на последующих (шестом и седьмом) шагах алгоритма, затем на восьмом, девятом и десятом шагах проявление виртуальной последовательности не будет наблюдаться и т.д.

Так, для $i=10$ в самом неблагоприятном случае будет иметь место такая закономерность: на шестом и седьмом шагах будет действовать виртуальная последовательность, на восьмом, девятом и десятом шагах алгоритма проявление виртуальной последовательности не будет наблюдаться.

Действуя на этих шагах классическим алгоритмом поиска, разобъём полуоткрытый интервал неопределенности $\left[x^1_1,1\right)$ на 2^3 равные части. По этой причине

$$l\left(\left[x^1_1,1\right)\right)=8h. \qquad (4)$$

По такой же схеме находятся значения функции $\psi'_{2,3}(i-5,1)$ для других значений параметра i.

Для нахождения значений функции $\psi^{**}_{2,3}(i-3,1)$ необходимо исходить из такой схемы: пропустить четвёртый и пятый шаги алгоритма, на шестом и седьмом шагах применить классический алгоритм поиска, затем пропустить восьмой и девятый шаги алгоритма, а на последующих трёх шагах применить классический алгоритм поиска и т.д.

Так, для $i=10$ классический алгоритм поиска применяется на шестом, седьмом и десятом шагах алгоритма.

В результате такой модернизации классического алгоритма исходный интервал неопределенности $\left[x^1_1,1\right)$ будет разбит на восемь равных частей, что не противоречит соотношению (4). Для $i=10$ значение функции $\varphi^{3,1,2,\infty}_{2,3}(10-3,1)=2$ (см. предыдущие значения этой функции для $i=7$).

Поскольку все члены соотношения (3) определены, то на основании этого выражения устанавливаем:

$$\varphi^{3,1,2,\infty}_{2,3}(10,1)=2\min\left\{8,\max\left\{8,2\right\}\right\}=16.$$

По описанной схеме находятся значения функций $\psi'_{2,3}(i-5,1)$, $\psi^{**}_{2,3}(i-3,1)$ для произвольного i.

Рассмотрим другой пример построения помехоустойчивого алгоритма поиска, для которого характерны такие параметры:

$$l_1=1,\ l_2=2,\ H=3,\ k=3,\ a=\infty.$$

Для этого примера на основании соотношения (23) [1] записываем:

$$\varphi^{3,1,2,\infty}_{2,3}(1,3)=\varphi^{3,1,2,\infty}_{2,3}(2,3)=\ldots=\varphi^{3,1,2,\infty}_{2,3}(4,3)=1;$$
$$\varphi^{3,1,2,\infty}_{2,3}(5,3)=4.$$

Пусть $i=6$. Тогда в результате первого шага алгоритма, как это уже известно, может возникнуть один из исходов типа $a_0)$, $a_1)$ и $a_2)$ [1].

Рассмотрим решение каждого исхода в отдельности.

Для исхода типа $a_0)$ применяется смешанная стратегия: $x^2_1=0$; $x^2_2\in\left(0,x^1_1\right)$; $x^2_3=x^1_1$; $x\in[0,1)$.

Самым неблагоприятным будет случай, когда на втором шаге алгоритма возникает исход типа $b_2)$, а на третьем шаге — исход типа $b_3)$.

В такой ситуации на четвертом шаге алгоритма применяем смешанную стратегию вида:

$$x^4_1=x^1_1;\quad x^4_2,x^3_2\in\left(x^1_1,1\right).$$

Пусть на четвертом шаге (рассматриваем наихудший случай) возникает исход типа $x+\zeta(t)>x^1_1$.

На пятом шаге снова применяем смешанную стратегию: $x^5_1=x^1_1$, точки x^5_2,x^5_3 размещаем в выделенном на четвёртом шаге алгоритма полуоткрытом интервале неопределённости.

При этом могут возникнуть такие исходы:

$$x+\zeta(t)\ge x^1_1;\quad x+\zeta(t)<x^1_1.$$

Для первого исхода характерно действие виртуальной последовательности на первых шагах алгоритма. Поскольку третий, четвёртый и пятый шаги выполнялись в отсутствие очередного выброса виртуальной последовательности, то их результаты являются истинными, на шестом шаге в обязательном порядке проявится очередной выброс виртуальной последовательности. По этой причине на последнем шаге нет возможности применить клас-

сический алгоритм поиска (в условиях действия виртуальной последовательности такие шаги пропускаются). За четвёртый и пятый шаги алгоритма полуоткрытый интервал неопределённости $\left[x_1^1,1\right)$ будет разбит на девять равных частей.

Если же возникает второй исход, то это свидетельствует о том, что виртуальная последовательность действовала на третьем и четвёртом шагах алгоритма, на последнем шаге применяется классический алгоритм поиска. Поскольку за первых два шага алгоритма полуоткрытый интервал $\left[0,x_1^1\right)$ был разбит на две равные части, а за шестой шаг каждая из них может быть разбита на четыре равные части, то полуоткрытый интервал $\left[0,x_1^1\right)$ в самом наихудшем случае будет разбит на восемь равных частей.

Итак, если на первом шаге алгоритма возникает исход типа a_0) [1], а на третьем — исход типа b_3) [1], то исходный интервал неопределённости будет разбит на семьнадцать равных частей. Если на третьем шаге алгоритма возникает исход типа b_1) [1], то это свидетельствует о действии отрицательного выброса виртуальной последовательности на третьем шаге, в этом случае поиск в полуоткрытом интервале $(-\infty, 0)$ не выполняется.

Пусть по итогам выполнения первого шага алгоритма был сформирован исход типа a_1) [1]:

$$x+\zeta(t)\in\left[x_1^1,x_2^1\right),$$

на втором шаге, как известно, применяется смешанная стратегия: $x_1^2=x_1^1$, $x_2^2\in\left(x_1^1,x_2^1\right)$, $x_3^2=x_2^1$.

Предположим, что на втором шаге возникает исход типа b_2) [1] (рассматривается наихудший случай). Тогда на третьем шаге снова применяем смешанную стратегию известного вида.

Пусть по итогам выполнения третьего шага алгоритма возникает исход типа b_1) [1]. Тогда на четвертом шаге применяется такая смешанная стратегия:

$$x_3^4=x_1^1,\quad x_1^4,x_2^4\in\left(0,x_1^1\right).$$

Пусть на четвёртом шаге возникает исход $x+\zeta(t)<x_1^1$.

Тогда на пятом шаге снова применяем смешанную стратегию: $x_3^5=x_1^1$, точки x_1^5,x_2^5 размещаем в выделенном на четвёртом шаге алгоритма полуоткрытом интервале неопределённости.

При этом могут возникнуть исходы:

$$x+\zeta(t)\le x_1^1;\quad x+\zeta(t)>x_1^1.$$

Для првого исхода характерно действие виртуальной последовательности на двух первых шагах алгоритма; третий, четвёртый и пятый шаги выполнялись в отсутствие очередного выброса виртуальной последовательности, на шестом шаге снова будет наблюдаться виртуальная последовательность. За четвёртый и пятый шаги алгоритма в результате применения смешанной стратегии полуоткрытый интервал $\left[0,x_1^1\right)$ будет разбит на девять равных частей.

В том случае, когда возникает второй исход, это будет свидетельствовать о действии виртуальной последовательности на третьем и четвёртом шагах алгоритма. В такой ситуации (см. решение исхода типа a_0) [1]) полуоткрытый интервал неопределённости $\left[x_1^1,x_2^1\right)$ будет разбит на восемь равных частей.

Пусть по итогам выполнения третьего шага алгоритма возникает исход типа b_3) [1]. Тогда в полуоткрытом интервале $\left[x_2^1,1\right)$ применяется смешанная стратегия: $x_1^4=x_2^1$, $x_2^4,x_3^4\in\left[x_2^1,1\right)$.

Как было уже показано (см. решение исхода типа a_0)): полуоткрытый интервал неопределённости $\left[x_2^1,1\right)$ будет разбит на девять равных частей.

Поскольку $l([0,1))=l\left(\left[0,x_1^1\right)\right)+l\left(\left[x_1^1,x_2^1\right)\right)+l\left(\left[x_2^1,1\right)\right)$, то исходный интервал неопределённости $(0,1)$ будет разбит на двадцать шесть равных частей.

Нетрудно убедиться (следует исходить из симметрии исходов), что при появлении исхода типа a_1), для которого $x+\zeta(t)\in\left[x_2^1,x_3^1\right)$, и исхода типа a_2) исходный интервал $(0,1)$ в первом случае разбивается на двадцать шесть, а во втором — на семнадцать равных частей.

Поскольку в самом неблагоприятном случае исходный интервал неопределённости $(0,1)$ будет разбит на семнадцать равных частей, этим устанавливаем истинность соотношения $\varphi_{2,3}^{3,1,2,\infty}(6,3)=17$.

По такой же схеме строят алгоритм поиска и для других значений параметра i,k и параметров виртуальной последовательности l_1, l_2, a, H.

Литература: 1.*Алипов Н.В., Алипов И.Н., Литвинова Е.И.* Методы защиты информации в дискретном канале на основе помехоустойчивых к симметричным нерегулярным виртуальным помехам алгоритмов поиска точки с характерным признаком // Радиоэлектроника и информатика. 2001. № 3. С. 84-92.

Поступила в редколлегию 30.05.2001

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

Алипов Николай Васильевич, д-р техн. наук, профессор кафедры проектирования и эксплуатации электронных аппаратов ХНУРЭ. Научные интересы: алгоритмизация задач автоматизированного проектирования электронных вычислительных средств, защита информации. Адрес: Украина, 61166, Харьков, пр. Ленина, 14, тел. 40-94-94.

Алипов Илья Николаевич, канд. техн. наук ХНУРЭ. Научные интересы: защита информации. Адрес: Украина, 61166, Харьков, пр. Ленина, 14, тел. 40-94-94.

Литвинова Евгения Ивановна, канд. техн. наук, доцент кафедры проектирования и эксплуатации электронных аппаратов ХНУРЭ. Научные интересы: алгоритмизация задач автоматизированного проектирования электронных вычислительных средств. Адрес: Украина, 61166, Харьков, пр. Ленина, 14, тел. 40-94-94.

Ребезюк Леонид Николаевич, канд. техн. наук, доцент кафедры проектирования и эксплуатации электронных аппаратов ХНУРЭ. Научные интересы: защита информации, автоматизация проектирования электронных вычислительных средств. Адрес: Украина, 61166, Харьков, пр. Ленина, 14, тел. 40-94-94.