всегда доступными параметрами сети, такими как физическая скрость передачи данных каналом соединения, длительность передачи пакета между источником и получателем и др. Более того, настоящая модель может с успехом использоваться как составная часть комплексной модели [3-5] сети передачи данных, которая в свою очередь является эффективным инструментом, применяемым на фазе проектирования и эксплуатации компьютерных сетей.

Литература: 1. *Шевчук А.С., Гусак О.Ю.* Протокол TCP – модель, функции, спецификации //Компьютеры + Программы, 1996. N8. С.16-22. 2. *Schwartz M.* Telecommunication Networks: Protocols, Modeling and Analysis // Addison-Wesley, 1987. С.32-41. 3. *Шевчук А.С., Кобзев И.В., Гусак О.Ю.* К вопросту о построении математической модели локальной вычислительной сети // АСУ и приборы автоматики, 1997. N2. С.94-97. 4. *Gusak O., Dayar T.* A generalization of a TCP Model: multiple source-destination case with arbitrary LAN as the access network, Proceedings of The Fourth Symposium on Computer Networks (BAS'99), 20-21 May 1999, Istanbul, Turkey. P. 102-111. 5. *Gusak O.* An analytical model of a client-server system functioning on top of TCP, Proceedings of The Sixth International Conference on Distributed Multimedia Systems (DMS'99), July 26-30, 1999, Aizu, Japan. P. 212-213. 6. *Stevens W. R.* TCP/IP Illustrated, Volume 1, The Protocols // Addison-Wesley, 1994. 576 pp. 7. *Heyman D.P., Lakshman T.V., Neidhardt A. L.* A New Method for Analysing Feedback Protocols with Applications to Engineering Web Traffic over the Internet, Performance Evaluation Review, 1997. P. 24-38.

Поступила в редколлегию 02.07.99

Рецензент: д-р техн. наук Петров Э.Г.

Гусак Олег Юрьевич, аспирант факультета компьютерной инженерии Университета Билькента (Анкара, Турция). Научные интересы: компьютерные сети, программное обеспечение, моделирование. Адрес: Турецкая республика, Анкара, 06533, Университет Билкент, факультет компьютерной инженерии, e-mail gusak@cs.bilkent.edu.tr

Кобзев Игорь Владимирович, канд. техн. наук, доцент кафедры информационных систем и технологий в деятельности ОВД Университета внутренних дел. Научные интересы: стохастическое моделирование, программное обеспечение. Украина, 310166, Харьков, ул. Новгородская,44,кв.19,тел.30-71-75.

e-mail k_infsis@adm.univd.kharkov.ua

Руденко Диана Александровна, канд. техн. наук., ассистент кафедры применения ЭВМ ХТУРЭ. Научные интересы: управление сложными объектами, программное обеспечение. Адрес: Украина, 310012, Харьков, ул. К.Маркса, 13/15, кв.33, тел. 23-13-96.

УДК 681.3+681.5:007

СИНТЕЗ ПОМЕХОУСТОЙЧИВЫХ К НЕРЕГУЛЯРНЫМ ВОЗМУЩЕНИЯМ АЛГОРИТМОВ ПОИСКА ТОЧКИ ЭКСТРЕМУМА УНИМОДАЛЬНОЙ ФУНКЦИИ

АЛИПОВ Н.В., БУЛАХ Е.В.

Дальнейшее развитие нового направления в криптографии с использованием дискретных автоматов требует разработки алгоритмов поиска точки экстремума унимодальной функции при воздействии на процесс поиска возмущений с различными характерными признаками. В статье описывается разработка таких алгоритмов в условиях воздействия симметричного нерегулярного возмущения. Приводятся логические схемы построения алгоритмов, которые позволяют для конкретных параметров построить помехоустойчивые к симметричным нерегулярным помехам алгоритмы поиска точки и тем самым определить функционирование дискретных автоматов для систем защиты информации.

Новым в совершенствовании методов защиты информации при ее передаче является направление, связанное с использованием теории дискретных автоматов [1]. Нами получен ряд оригинальных результатов, изложенных в работе [2]. Основу предложенных методов составляют помехоустойчивые алгоритмы поиска точки экстремума в условиях воздействия на процесс поиска регулярных симметричных возмущений, так называемых $A_{2,8}$-последовательностей. Существуют и нерегулярные возмущения. В статье рассматриваются помехоустойчивые алгоритмы поиска точки экстремума в условиях воздействия на процесс поиска нерегулярных симметричных возмущений, так называемых $A_{2,3}$ - последовательностей. Характерной особенностью этих последовательностей является то, что длительность возмущения – случайная величина, распределенная по некоторому закону в интервале $[l_1, l_2)$, где l_1, l_2 - соответственно минимально и максимально возможные значения длительности возмущения.

Рассмотрим помехоустойчивые к $A_{2,3}(a, l_1, l_2, H)$ –последовательности алгоритмы поиска точки экстремума унимодальной функции.

Пусть $H > l_2$ и некоторым образом выбрана точка первого эксперимента. Тогда на первом шаге алгоритма (это уже известно [2]) может появиться один из исходов типа a).

Применяя на втором шаге алгоритма к этому исходу смешанную стратегию [2], получаем один из исходов:

$$b_1)\ f\left(x_1^2\right) = \max_{\rho}\left\{f\left(x_\rho^2\right)\right\}$$

$$b_2)\ f\left(x_{q1}^2\right) = \max_{\rho}\left\{f\left(x_\rho^2\right)\right\} q_1 = \overline{2,\ k-1};$$

$$b_3)\ f\left(x_k^2\right) = \max_{\rho}\left\{f\left(x_\rho^2\right)\right\}$$

Исход b_1) свидетельствует о действии $A_{2,3}$-последовательности на одном из первых шагов алгоритма. На последующих $(k-1)$-шагах применяют в полуоткрытом интервале $\left[x_{q-1}^{1,1}, x_2^2\right)$ непомехоустойчивый алгоритм поиска.

Затем на (l_1+2)-м шаге организуют проверку правильности формирования исхода типа b_1). С этой целью, как известно [2], одну точку эксперимента размещаем в точке x_q^1, остальные – в выделенном на (l_1+1)-шаге алгоритма интервале неопределенности. При этом могут возникнуть исходы:

$$b_1^1)\ f(x_{q2}^{l+2}) = \max_{\rho} f(x_{\rho}^{l+2}),\ q_2 = \overline{1, k-1};$$

$$b_1^2)\ f(x_k^{l+2}) = \max_{\rho} f(x_{\rho}^{l+2}).$$

Для исхода типа b_1^1) нельзя однозначно утверждать, что: прекратилось действие $A_{2,3}$-последовательности (длительность импульса $A_{2,3}$-последовательности принадлежит диапазону $[l_1, l_2]$).

Если же на (l_1+2)-м шаге формируется исход типа b_1^2), то это свидетельствует о том, что $A_{2,3}$-последовательность аддитивно наложилась на координату точки экстремума на втором, третьем, ... , (l_1+1)-м шагах алгоритма и на последующих (l_2-1) шагах алгоритма будет отсутствовать, затем снова проявится на l_3 шагах алгоритма $(l_3 \in [l_1, l_2])$ и т.д.

По этой причине в случае формирования исхода b_1^1) снова принимают смешанную стратегию (l_1+2)-го шага алгоритма.

На (l_1+3)-м шаге алгоритма сможет быть сформирован один из исходов типа b_1^1) и b_1^2).

Если на (l_1+3)-м шаге формируется исход типа b_1^2), то это свидетельствует о том, что $A_{2,3}$-последовательность действовала на втором, третьем, ... , (l_1+2)-м шагах алгоритма. Поскольку проявление $A_{2,3}$-последовательности обнаружено, то в дальнейшем применяют известный способ в полуоткрытом интервале неопределенности $[x_{q-1}^1, x_{q+1}^1)$.

Если на (l_1+3)-м шаге алгоритма снова возникает исход типа b_1^1), то применяют к выделенному на этом шаге алгоритма смешанную стратегию (l_1+2)-го шага алгоритма.

Наихудшим будет случай, когда исход типа b_1^1) возникает на (l_1+2)-м, (l_1+3)-м, ... , (l_2+2) шагах алгоритма.

Пусть на (l_2+2)-м шаге алгоритма формируется исход типа b_1^1). Тогда это будет свидетельствовать о том, что $A_{2,3}$-последовательность действовала на первом шаге алгоритма и не будет еще проявляться на (l_1-l_2-1)шагах алгоритма, затем проявится снова на l_3-х шагах алгоритма $(l_3 \in [l_1, l_2])$ и т.д.

Если же по итогам выполнения (l_2+2)-го шага алгоритма будет сформирован исход типа b_1^2), то $A_{2,3}$-последовательность действовала на втором, третьем, ... , (l_2+1)-м шагах алгоритма и на последующем (l_1-1)-м шаге алгоритма она не будет проявляться, затем снова проявится на l_3-х шагах алгоритма и т.д.

Стратегия поиска для рассмотренных исходов состоит в том, что поиск точки экстремума унимодальной функции будет осуществляться на тех шагах алгоритма, на которых проявление $A_{2,3}$-последовательности отсутствует.

Применяя описанную схему поиска интервала неопределенности $[x_{q-1}^{1,1}, x_2^2)$, разобьем в наихудшем случае на $\overline{\varphi}_{2,3}^{\,l_1,l_2,H}(l_1, k)$ равных частей:

$$\overline{\varphi}_{2,3}^{\,l_1,l_2,H}(l_1, k) = \varphi(l_1-1, k)\times\varphi(l_2-l_1+1)\,k-1)\,\varphi(l_1, k), \quad (1)$$

где $\varphi(l_1-1, k)\ \varphi(l_2-l_1+1)\,k-1)$, $\varphi(l_1, k)$ – количество равных частей, которые разбивают помехоустойчивый алгоритм поиска соответственно за (l_1-1) шагов, формируя k точек эксперимента, за (l_2-l_1+1) шагов, формируя (l_2-1)-ю точку эксперимента, за i_1 шагов, формируя k точек эксперимента:

$$i_1 = (l_2-l_1-1)+(l_1-1)\alpha+\alpha_1;$$

$$\alpha = \begin{cases} \dfrac{i-1-H}{l_2+H}, & (i-1-H) \bmod (l_2+H) = 0; \\ \left[\dfrac{i-1-H}{l_2+H}\right], & (i-1-H) \bmod (l_2+H) \neq 0; \end{cases} \quad (2)$$

$$\alpha_2 = \begin{cases} 0, & (i-1-H) \bmod (l_2+H) = 0, \ \textit{либо} \\ (i-1-H) \bmod (l_2+H), & (i-1-H) \bmod (l_2+H) \leq l_2; \\ l_2, & (i-1-H) \bmod (l_2+H) > l_2. \end{cases}$$

Для b_1^2) исходный полуоткрытый интервал неопределенности $[x_{q-1}^1, x_{q+1}^1)$ будет разбит на $\varphi(l_2, k)$ равные части:

$$\alpha_2 = \begin{cases} \dfrac{i-l_2-H}{l_2+H}, & (i-l_2-H) \bmod (l_2+H) = 0; \\ \left[\dfrac{i-l_2-H}{l_2+H}\right], & (i-l_2-H) \bmod (l_2+H) \neq 0, \end{cases}$$

где $i_2 = (l_2-1)+(l_2-1)\alpha_2+\alpha_3$,

$$\alpha_3 = \begin{cases} 0, & (i-l_2-H) \bmod (l_2+H) = 0, \ \textit{либо} \\ (i-l_2-H) \bmod (l_2+H), & (i-l_2-H) \bmod (l_2+H) \leq l_2; \\ l_2, & (i-l_2-H) \bmod (l_2+H) > l_2. \end{cases}$$

Если при выполнении второго шага алгоритма сформирован исход типа b_3), то разрешают таким же образом как и исход типа b_1). В этом случае точки третьего эксперимента размещают в полуоткрытом интервале $[x_{k-1}^2, x_{q+1}^{1,2})$. Процесс поиска на третьем, ..., (l_1+1)-м шаге организуют по той же схеме, что и для исхода типа b_1). На (l_1+2)-м шаге алгоритма применяют смешанную стратегию такого вида:

$$x_1^{l_1+2} = x_q^1;\ x_{q1}^{l_1+2} \in [x_{q2-1}^{l_1+1}, x_{q2+1}^{l_1+1}), \quad (3)$$

где $q_1 = \overline{2,k}$, $\left[x_{q2-1}^{l1+1}, x_{q2+1}^{l1+1}\right($ – полуоткрытый интервал неопределенности, выделенный на $(j+1)$ шаге алгоритма $q_2 = \overline{1,k}$.

В наихудшем случае полуоткрытый интервал неопределенности $\left[x_{k-1}^{2}, x_{q+1}^{1,2}\right($ будет разбит на $\varphi_{2,3}^{l_1,l_2,H}(j, k)$ равных частей. Для функции $\varphi_{2,3}^{l_1,l_2,H}(j, k)$ имею место соотношения (1), (2).

Если в процессе поиска формируется исход типа b_2), то применяют в этом случае смешанную стратегию исхода типа a).

Если исход типа b_2) появился на первых j-х шагах алгоритма $(j \le H)$, и на j-м шаге алгоритма относительно точки экстремума унимодальной функции выделен полуоткрытый интервал неопределенности $\left[x_{q_{j+1}-1}^{j+1}, x_{q_j+1}^{j,2}\right($, то в случае формирования исхода типа b_1) либо b_3) полуоткрытые интервалы неопределенности $\left[x_{q_{j+1}-1}^{j+1}, x_2^{j+1}\right($, $\left[x_{q_{j+1}-1}^{j+1}, x_{q_j+1}^{j,2}\right($ в наихудшем случае будут разбиты на $\varphi_{2,3}^{l_1,l_2,H}(j, k)$ равных частей:

$$\varphi_{2,3}^{l_1,l_2,H}(j, k) = \varphi(j-1, k) \times \varphi(i_3 - l_1 + 1) \times \varphi(j, k), \quad (4)$$

$$i_3 = (j - l_2 - 1) + (j - 1)\alpha + \overline{\alpha}_1,$$

$$\overline{\alpha} = \begin{cases} \dfrac{j - j - l_2 - H}{l_2 + H}, & (j - j - l_2 - H) \bmod (l_2 + H) = 0; \\ \left\lfloor \dfrac{j - j - l_2 - H}{l_2 + H} \right\rfloor, & (j - j - l_2 - H) \bmod (l_2 + H) \neq 0, \end{cases}$$

$$\alpha_3 = \begin{cases} 0, & (j - j - l_2 - H) \bmod (l_2 + H) = 0, \textit{ либо} \\ (j - j - l_2 - H) \bmod (l_2 + H), & (j - j - l_2 - H) \bmod (l_2 + H) \le l_2; \\ (j - j - l_2 - H) \bmod (l_2 + H) - l_2, & (j - j - l_2 - H) \bmod (l_2 + H) > l_2. \end{cases}$$

Как известно, начиная с $(j + 1 + l_1)$-го и заканчивая $(j + l_2 + 1)$-м шагом применяется смешанная стратегия, задаваемая соотношением (3).

При этом могут возникнуть исходы типа b_1^1), b_1^2) либо типа b_3^1), b_3^2).

Если возникает исход типа b_1^1) или типа b_3^1), то исходные для них интервалы неопределенности будут соответственно разбиты на $\varphi_{2,3}^{l_1,l_2,H}(j, k)$ равные части (см. соотношение (4)). В том случае когда исход типа b_1^2) или типа b_3^2) возникает на $(j + 1 + l_2)$-м шаге алгоритма, интервал неопределенности $\left[x_{q-1}^{j}, x_{q+1}^{j}\right($ будет разбит на $\varphi_{2,3}^{*}(j - j, k)$:

$$\varphi_{2,3}^{*}(j - j, k) = \varphi(j - 1, k - 1) \times \varphi(i_4, k),$$

$$i_4 = (j - 1) + (j - 1)\alpha_2 + \overline{\alpha}_3,$$

$$\overline{\alpha}_2 = \begin{cases} \dfrac{j - j - l_2 - H}{l_2 + H}, & (j - j - l_2 - H) \bmod (l_2 + H) = 0; \\ \left\lfloor \dfrac{j - j - l_2 - H}{l_2 + H} \right\rfloor, & (j - j - l_2 - H) \bmod (l_2 + H) \neq 0; \end{cases}$$

$$\overline{\alpha}_3 = \begin{cases} 0, & (j - j - l_2 - H) \bmod (l_2 + H) = 0, \textit{ либо} \\ (j - j - l_2 - H) \bmod (l_2 + H), & (j - j - l_2 - H) \bmod (l_2 + H) \le l_2; \\ (j - j - l_2 - H) \bmod (l_2 + H) - l_2, & (j - j - l_2 - H) \bmod (l_2 + H) > l_2. \end{cases}$$

Если же при выполнении $(j+1)$-го шага алгоритма вновь возникает исход типа b_2) и при этом $(j+1) < (l_2 + 1)$, то его разрешают известным способом (применяют смешанную стратегию).

Если же при выполнении $(j+1)$-го шага возникает исход типа b_2) и справедливо соотношение $(j+1) = (l_2 + 1)$, то это свидетельствует о том, что $x^* \in \left[x_{q-1}^{1}, x_{q+1}^{1}\right($.

Если же на $(j+1)$-м шаге возникает исход типа b_2) и истинным будет такое соотношение $(j+1) = H$, то это свидетельствует о том, что на первых шагах алгоритма не было проявления $A_{2,3}$ - последовательности. По этой причине $x^* \in \left[x_{q_{j+1}-1}^{j+1}, x_{q_{j+1}}^{j+1}\right($, где $q_{j+1} = \overline{1,k}$.

Этот полуоткрытый интервал неопределенности будет за $(j+1)$-й шаг разбит на $\varphi(j+1, k-1)$ равные части, где $\varphi(j+1, k-1)$ – оценка непомехоустойчивого алгоритма.

Запишем очевидные соотношения:

$\varphi_{2,3}^{l_1,l_2,H}(1, k) = \ldots \varphi_{2,3}^{l_1,l_2,H}(l_2, k) = 1$,

$\varphi_{2,3}^{l_1,l_2,H}(l_2 + 1, k) = (j+1) \cdot 2$ (k-нечетное число).

Описанные стратегии поиска и правила формирования нового интервала неопределенности позволяют методом индукции построить алгоритм для любых его параметров и любых параметров $A_{2,3}$ - последовательности и тем самым разработать оригинальные методы защиты информации при ее передаче.

Литература: 1. *Алипов И.Н., Ребезюк Л.Н.* Постановка задач синтеза новых методов защиты информации // Радиотехника. Вып. 103. С. 60-64. 2. *Булах Е.В.* Методы защиты информации на основе деревообразных автоматов / Зб. наукових праць за матеріалами 3-го міжнародного молодіжного форуму "Радіоелектроніка і молодь у XXI ст.", ч. 2. Х.: ХТУРЕ, 1999. 502 с.

Поступила в редколлегию 19.09.99

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

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

Булах Евгений Вячеславович, аспирант кафедры конструирования электронно-вычислительных машин ХТУРЭ. Научные интересы: защита информации. Адрес: Украина, 310007, Харьков, пр.50 лет ВЛКСМ, 65-а, кв. 8, тел. 40-94-94.