

острых респираторно-вирусных или обострения стрептококковых инфекций в патологический процесс вовлекаются суставы. Если очаги инфекции не были своевременно выявлены и санированы, то ГВ протекает всегда с рецидивами

Снизить риск развития ГВ, можно путем проведения первичной профилактики: рациональное питание, выявление очагов хронической инфекции и своевременное эффективное их лечение во все возрастные периоды, выполнение широкого комплекса санитарно-гигиенических правил, исключение факторов, провоцирующих заболевание (переохлаждение, гиперинсоляция, физические и психические перегрузки).

ВЫСОКИЕ ДОЗЫ МЕТОТРЕКСАТА И СИСТЕМА ГЕМОСТАЗА У ДЕТЕЙ С ОСТРЫМ ЛИМФОБЛАСТНЫМ ЛЕЙКОЗОМ

Рошик А.С., Колесникова О.И.

Алтайский государственный медицинский университет, Барнаул, e-mail: roanse@bk.ru

Метотрексат – один из ключевых препаратов, применяемый в различных протоколах лечения онкогематологических заболеваний, так при остром лимфобластном лейкозе (ОЛЛ) его применяют на протоколе М в высоких дозах – 1 г/м², что приводит, как известно, к поражениям кожи, печени, нейротоксичности, угнетению костномозгового кроветворения. Однако сведений о влиянии высоких доз метотрексата на свертывающую активность крови и фибринолиз у детей с ОЛЛ недостаточно.

Цель исследования было изучить состояние коагуляционного звена гемостаза и фибриноли-

за на фоне проведения высокодозного метотрексата (протокол М) у детей с ОЛЛ.

Обследовано 45 больных с ОЛЛ в возрасте от 1 года до 14 лет. Исследование системы гемостаза проводилось следующими методиками: активированное парциальное тромбопластиновое время, протромбиновое, тромбиновое, эхитоксовое время, уровень фибриногена, уровень растворимых фибрин-мономеров, определение антитромбина III, протеинов S и C, XII-а зависимый лизис эуглобулинов, определение уровня плазминогена, определение уровня D-димера, количество тромбоцитов. Исследование проводилось на фоне проведения высокодозной химиотерапии.

У 50% детей с ОЛЛ перед проведением протокола М отмечался геморрагический синдром, сопровождающийся гипокоагуляцией во всех коагуляционных тестах, тромбинемией, угнетением фибринолиза при нормальных показателях фибриногена и антитромбина III, протеинов S и C, плазминогена. На фоне лечения геморрагический синдром не нарастал, выявлены удлинение времени свертывания в эхитоксовом тесте, снижение фибриногена, физиологических антикоагулянтов – антитромбина III, протеинов S и C, при сохранении гипокоагуляции в других тестах, тромбинемии и угнетении фибринолиза.

Полученные данные свидетельствуют о том, что у детей с ОЛЛ на фоне лечения высокодозным метотрексатом развивается тромбофилия, обусловленная дефицитом физиологических антикоагулянтов, что является фактором протромбогенного риска. Необходимо исследование системы гемостаза в динамике для диагностики этих нарушений и своевременной их коррекции.

«Научные исследования высшей школы по приоритетным направлениям науки и техники», Швейцария (Берн), 27 апреля – 3 мая 2014 г.

Технические науки

КРИПТОГРАФИЧЕСКИЕ СИСТЕМЫ УПРАВЛЕНИЯ ДЕТЕРМИНИРОВАННЫМ ХАОСОМ

Когай Г.Д., Тен Т.Л., Газалиева М.А., Шкурапет К.В.

КарГТУ «Карагандинский Государственный технический университет», Караганда, e-mail: tentl@mail.ru

Из теории динамических систем [1-4] известен такой факт, что для достаточно общих семейств хаотических динамических систем существуют периодические возмущения, приводящие к стабилизации цикла заданного периода. Предлагаемый криптографический метод базируется на этом факте. Информация шифруется с помощью такого метода. В качестве пере-

даваемого сигнала используются возмущения, а ключом для расшифровки полученного сообщения служит вид отображения (т.е. вид функции, задающей отображение).

Цель. Разработать криптографический метод на основе стабилизации хаотического поведения динамической системы. Провести исследование данного криптографического метода по всем необходимым параметрам.

Описание. Рассмотрим основные положения и результаты, полученные в теории динамических систем относительно стабилизации хаотического поведения. В настоящее время наиболее успешными методами стабилизации поведения (т.е. управления поведением) динамических систем являются метод мультипликативного воздействия с обратной связью и метод

без обратной связи [4, 5]. Предположим, что рассматриваемая система задается обыкновенными дифференциальными уравнениями следующего вида:

$$\dot{x} = v(x, a), \quad (1.1)$$

где $x = \{x_1, \dots, x_n\}$ – совокупность динамических переменных, $v = \{v_1, \dots, v_n\}$ – некоторая n -компонентная нелинейная функция и a – управляющий параметр. Проблема управления поведением системы (1.1) заключается в том, чтобы найти такое внешнее возмущение G , при котором фазовый поток $F^t(x, G)$, порождаемый возмущенной динамической системой

$$\dot{x} = v'(x, a, G) \quad (1.2)$$

стремился бы к выбранному подмножеству $A(G)$ ее фазового пространства.

Подмножество $A(G)$ может быть как аттрактором, так и неустойчивым множеством. В последнем случае возмущения G модифицируют систему (1.1) таким образом, что фазовые траектории подходят к подмножеству $A(G)$ и остаются в достаточно малой его окрестности $U \supset A(G)$ под действием G .

Если внешние возмущения реализуются посредством мультипликативного воздействия по отношению к динамическим переменным x , то говорят, что имеет место параметрическое (или мультипликативное) управление, поскольку, как правило, параметры мультипликативно включаются в динамическую систему.

В этом случае регулирование состоит в такой модификации функции v в соотношении (1.1), чтобы новая система $\dot{x} = v'(x, a', t)$ имела бы требуемое (заранее выбранное) поведение. Здесь $v'(x, a', t) = v(x, a_0 + a_1(t))$ и параметр $a_1(t)$ обычно является Т-периодической функцией.

Для параметрических возмущений с обратной связью учитывается текущее состояние системы: $v'(x, a', t) = v(x, a(x(t)))$. В этом случае параметр должен изменяться специальным путем, и необязательно периодически.

Достаточно часто в приложениях встречается ситуация, когда мультипликативное введение внешних возмущений в систему невозможно. Тогда фазовый поток $F^t(x, G)$, раскладывается на две составляющие: часть, соответствующую невозмущенному фазовому потоку $F^t(x)$, и компоненту $F^t(G)$, которая инициируется исключительно возмущениями $F^t(x, G) = F^t(x) + F^t(G)$. В этом случае имеет место аддитивное возмущение, т.е. $v'(x, a', t) = v(x, a) + g(t)$, где $g(t)$ обозначает внешнее воздействие. Таким образом, управление динамикой системы подразумевает приложение силовой компоненты к векторной функции. Поэтому данный тип управления поведением динамической системы называется силовым. В свою очередь, если в силовом кон-

троле учитывается обратная связь, то функция v модифицируется как $v'_i = v_i(x, a) + g_k(x_i(t))$, $i = 1, 2, \dots, n$, $1 \leq k \leq n$.

По ряду причин параметрический метод стабилизации динамики имеет определенные преимущества перед силовым. Во-первых, в приложениях к физическим, химическим и другим важным системам часто рассматриваются величины, которые являются пропорциональными динамическим переменным x_i . Для таких систем $v(0, a_1, \dots, a_m) = 0$, а гиперповерхности x_i являются инвариантными множествами. Это означает, что система (1.1) отражает реальные процессы только на симплексе $X = \left\{ x \mid x_i > 0, \sum_{i=1}^n x_i < const \right\}$.

В этом случае внешнее аддитивное воздействие может привести к тому, что фазовые траектории покинут множество X , пересекая гиперповерхности $x_j = 0$. Поэтому силовое воздействие может явиться причиной вырождения системы или выхода ее на нежелательный режим эволюции. Например, для биологических систем это означает вымирание части особей. В то же время, параметрическое воздействие означает изменение ресурсов системы и, таким образом, является более тонким в сравнении с силовым. Во-вторых, силовое возмущение гораздо труднее реализовать. Так, для химических систем силовой контроль подразумевает введение (и соответственно, удаление) дополнительных веществ; для биологических систем такой метод стабилизации может быть реализован через стерилизацию части особей или введением в сообщество дополнительных видов. С другой стороны, в противоположность параметрической стабилизации, силовой метод, как правило, приводит к требуемому результату для почти всех систем, поскольку во многих случаях ее естественное поведение может быть буквально «задавлено» внешней силой. Введение обратной связи является определенным преимуществом, поскольку в большинстве случаев такой способ управления приводит к требуемому результату: выбранный заранее седловой предельный цикл стабилизируется и, таким образом, исследуемая система выводится на требуемый режим движения. Однако этот метод эффективен, если только изображающая точка находится вблизи выбранного цикла. В противном случае необходимо использовать дополнительные способы воздействия. В то же время методы стабилизации без обратной связи не требуют введения постоянного компьютерного (или какого-либо другого) слежения за состоянием системы и менее подвержены воздействиям шумов, что существенно упрощает их использование в приложениях.

Основные результаты, полученные в теории динамических систем и относящиеся к стабилизации хаотического поведения внешними возмущениями без обратной связи, сводятся к сле-

дующему [5, 6]. Пусть задана динамическая система (отображение) $T_a: M \rightarrow M$,

$$T_a: x \mapsto f(x, a), \quad (1.3)$$

где $a \in A \subset \mathbb{R}$ и $f = \{f_1, \dots, f_n\}$, $x = \{x_1, \dots, x_n\}$. Допустим, что эта система при определенных значениях параметра может иметь хаотическое поведение, т.е. существует некоторое подмножество A_c , $A_c \subset A$, такое, что для $a \in A_c$ динамика (1.3) (возможно, при некоторых начальных условиях) отлична от стационарной, периодической и квазипериодической. Для стабилизации хаотического поведения необходимо определить такое возмущение G , действующее на хаотическом множестве A_c , $G: A_c \rightarrow A_c$,

$$G: a \mapsto g(a), a \in A_c, \quad (1.4)$$

$$A_c = \{\hat{a} \in A_c \otimes A_c \otimes \dots \otimes A_c : \hat{a} = (a_1, \dots, a_\tau), a_i \neq a_j, 1 \leq i, j \leq \tau, i \neq j, a_1, \dots, a_\tau \in A_c\}$$

$A_c \subset \mathbb{R}^\tau$, отвечающее всевозможным воздействиям периода t , оперирующим в A_c .

В работах [6, 7] было показано, что среди наборов $\{\hat{a}\} = \{a_1, a_2, \dots, a_\tau\}$, составляющих множество A_c , существуют такие $\{a_1^d, a_2^d, a_\tau^d\} = A_d \subset A_c$, что отображение (1.5) обладает устойчивыми циклами конечных периодов, причем период t полученного устойчивого цикла всегда кратен периоду возмущения, $t = \tau k$, где $k = 1, 2, \dots$. Такая ситуация оказывается типичной для большого класса хаотических отображений [8-10]. Более того, для любого семейства унимодальных и кусочно-линейных отображений возможно найти такие возмущения a_1, a_2, \dots, a_p , при которых соответствующие возмущенные семейства обладают устойчивыми циклами с предписанными периодами.

Этот результат основан на следующем свойстве: если для отображения $T_a: x \mapsto f(x, a)$, $x \in M$, $a \in A$, существует подмножество $\sigma \in M$ такое, что для любых $x_1, x_2 \in \sigma$ найдется $a^* \in A$, для которого $f(x_1, a^*) = x_2$ и имеется критическая точка $x_c \in \sigma$ такая, что $\partial f(x, a) / \partial x|_{x=x_c} \equiv D_x f(x_c, a) = 0$ при любом $a \in A$, то для любых $x_2, x_3, \dots, x_t \in \sigma$, $t = \tau$, существуют такие x_1 и a_1, a_2, \dots, a_t , что цикл (x_1, x_2, \dots, x_t) $t = \tau$, будет устойчивым циклом возмущенного отображения T_a при параметрических возмущениях a_1, a_2, \dots, a_t .

В общем случае подмножество A_d , соответствующее стабилизированному поведению, имеет достаточно сложную структуру [9, 10]. Однако для квадратичного семейства

$$T_a: x \mapsto ax(1-x), \quad (1.6)$$

с периодическим возмущением (a_1, a_2, \dots, a_t) подмножество A_d , отвечающее циклам периода $t = \tau$ оказывается целой областью и разбивается на такие подобласти, что возмущения из каждой такой подобласти приводят к стабилизации цикла определенного периода. Именно этот результат и позволяет эффективно использовать дан-

чтобы результирующая возмущенная динамическая система

$$T_a: \begin{cases} x \mapsto f(x, a), \\ a \mapsto g(a), x \in M, a \in A_c, \end{cases} \quad (1.5)$$

обладала устойчивыми циклами. При периодическом возмущении преобразование G , задающее закон изменения параметров, определено лишь в конечном наборе точек $\{a_1, a_2, \dots, a_t\}$ причем $a_{i+1} = g(a_i)$, $i=1, 2, \dots, t-1$, и $a_1 = g(a_t)$, $a_1, a_2, \dots, a_t \in A_c$. В этом случае удобно каждому возмущению периода t параметра поставить в соответствие вектор $\hat{a} = (a_1, \dots, a_t)$ из пространства \mathbb{R}^τ .

Тогда можно рассмотреть множество

ное отображение для шифрования и пересылки скрытых сообщений.

Рассмотрим подробнее периодически (с периодом t) возмущенное семейство (1.6). Его удобно переписать в следующем виде:

$$\begin{cases} x_{n+1} = a_n x_n (1 - x_n), \\ a_n = a_{n \bmod \tau + 1} \end{cases} \quad (1.7)$$

Если это отображение имеет цикл периода $t = \tau$, $p = (x_1, x_2, \dots, x_t)$, то точки этого цикла будут удовлетворять следующей системе уравнений

$$\begin{cases} x_2 = a_1 x_1 (1 - x_1), \\ x_3 = a_2 x_2 (1 - x_2), \\ \dots, \\ x_1 = a_t x_t (1 - x_t). \end{cases} \quad (1.8)$$

Для решения обратной задачи, т.е. нахождения значений параметров, при которых отображение (1.7) имеет заданный цикл $p = (x_1, x_2, \dots, x_t)$, необходимо выразить a_i из системы (1.8):

$$\begin{aligned} a_1 &= \frac{x_2}{x_1(1-x_1)}, \\ a_2 &= \frac{x_3}{x_2(1-x_2)}, \\ a_t &= \frac{x_1}{x_t(1-x_t)}. \end{aligned} \quad (1.9)$$

Очевидно, что при этом не для всех $x_i \in (0, 1)$ имеет место $a_i \in [0, 4]$. Однако при выполнении этого условия для любого цикла $p = (x_1, x_2, \dots, x_t)$ найдутся такие параметры (a_1, a_2, \dots, a_t) , при которых возмущенное отображение (1.7) будет обладать циклом p . При

$$|\beta(p)| \equiv \left| \prod_{i=1}^t a_i (1 - 2x_i) \right| < 1$$

он будет устойчив.

С учетом равенств (1.9) это условие переписывается как:

$$|\beta(p)| = \left| \prod_{i=1}^l \frac{x_{i+1}}{x_i(1-x_i)} (1-2x_i) \right| = \left| \prod_{i=1}^l \frac{1-2x_i}{1-x_i} \right| < 1. \quad (1.10)$$

Поскольку при $x_c = 1/2$ имеем $(1-2x_c)/(1-x_c) = 0$, то неравенство (1.10) всегда может быть выполнено. Множество значений (x_1, x_2, \dots, x_l) , при которых $a_i \in [0, 4]$ и удовлетворяется неравенство (1.10), образует в пространстве R^l определенную область, каждая точка которой соответствует устойчивому циклу возмущенного отображения. Преобразуя эту область при помощи системы (1.9), получим соответствующую область значений параметров в параметрическом пространстве R^l .

Предлагаемый криптографический метод на основе стабилизации хаотического поведения динамических систем и будет использоваться в качестве основополагающего начала для разработки алгоритмов криптографического преобразования информации на базе хаотического отображения.

Вывод. Предлагаемый криптографический метод базируется на таком известном факте из теории динамических систем: для достаточно общих семейств хаотических динамических систем существуют периодические возмущения, приводящие к стабилизации цикла заданного периода. Информация шифруется с помощью таких стабилизированных циклов. В качестве передаваемого сигнала используются возмущения, а ключом для расшифровки полученного сообщения служит вид отображения.

В настоящее время имеются программные средства, реализующие криптографический ме-

тод на основе стабилизации хаотического поведения динамических систем [11].

Список литературы

1. Лоскутов А.Ю., Рыбалко С.Д., Чураев А.А. Система кодирования информации посредством стабилизации циклов динамических систем: Письма в ЖТФ, 2004, т. 30, вып.20. – С.1-7.
2. Лоскутов А.Ю., Петренко Е.О., Рыбалко С.Д., Чураев А.А. Разработка системы кодирования информации, осуществляемого на основе стабилизации циклов отображений нелинейных динамических систем // Научная сессия МИФИ-2004: Сборник научных трудов в 15 томах. Т.2. Программное обеспечение. Информационные технологии. – М.: МИФИ, 2004.
3. Proc. Of the SPIE 1993 Annual Meeting «Chaos in Communication». – San Diego California, 11-16 July, 1993, v. 2038.
4. Дмитриев А.С. Запись и распознавание информации в одномерных динамических системах. – Радиотехника и электроника, 1991, т. 5. – С. 101-108.
5. Loskutov A.Y., Shishmarev A.I. Control of dynamical systems behavior by parametric perturbations an analytic approach. – Chaos, 1994, v.4, No2, p. 351-355.
6. Бейсенби М.А., Ойнаров А.Р. Детерминированный хаос в развитии экономической системы. – Проблемы автоматки и управления. Институт автоматки НАН КР. – Бишкек, Илим, 2007, с. 37-40.
7. Тен Т.Л., Бейсенби М.А., Когай Г.Д. Разработка системы защиты информации в распределенных сетях: Монография. – Караганда: КарГТУ, 2012. – С.193-197.
8. Алексеев В.В., Лоскутов А.Ю. Управление системой со странным аттрактором посредством периодического параметрического воздействия. – ДАН СССР, 1987, Т.293, вып.6. – С. 1346-1348.
9. Loskutov A.Y., Tereshko V.M., Vasiliev K.A. Stabilization Of Chaotic Dynamics One-dimensional maps by cyclic parametric transformation – Int. J. Bi./ and Chaos, 1996, v.6, No4. – P. 725-735.
10. Marino I.P., Lopez L., Sanjuan M.A.F. Channel coding in communications using chaos //Physics Letters A. 2002. 295. – P. 185-191.
11. Бейсенби М.А., Тен Т.Л., Когай Г.Д. Управление детерминированным хаосом в распределенных сетях: Учебное пособие. – Караганда, КарГТУ, 2013. – С. 113-124.