Lucks. Attacks on AURORA-512 and the Double-MIX Merkle-Damgard Transform // Режим доступу до ресурсу – http://eprint.iacr.org/2009/113.pdf **7.** E. Fleischmann, M. Gorski, S. Lucks. On the Security Of Tandem-DM. Full version of paper (2009/02/03) // Режим доступу до ресурсу – http://eprint.iacr.org/2009/054.pdf **8.** Патент України на корисну модель № 18693 МПК G 09 C 1/00. Спосіб ключового хешування теоретично доведеної стійкості / Стасєв Ю. В., Кузнецов О. О., Євсеєв С. П., Чевардін В. Є., Малахов С. В., Гришко А. В.; заявник та патентовласник Харківський університет повітряних сил. – №u200605734 ; заявл. 25.05.06 ; опубл. 15.11.06, Бюл. № 11.

УДК 621.391

ИСПОЛЬЗОВАНИЕ BDS-СТАТИСТИКИ ДЛЯ ОЦЕНКИ ПАРАМЕТРОВ ОДНОМЕРНЫХ ОТОБРАЖЕНИЙ ПО НАБЛЮДЕНИЮ ХАОТИЧЕСКОГО ВРЕМЕННОГО РЯДА

Константин Васюта
Харьковский университет Воздушных Сил

Аннотация: **Для анализа структурной скрытности систем передачи информации с хаотической несущей, формируемой одномерным отображением, предложен новый метод оценки его параметров с использованием непараметрической BDS-статистики. В работе показано, что, опираясь на различие в топологических свойствах в фазовом пространстве хаотических, регулярных и случайных процессов с независимыми значениями можно решать задачу оценки параметров отображения по наблюдению хаотического временного ряда на фоне белого шума. Приведены результаты численного моделирования предложенного метода оценки параметров хаотических отображений для различного характера шума.**
Summary: **For the analysis of structural stealthiness of transmission systems of the information with random bearing, shaped one-dimensional representation, offers a new method of an estimate of its parameters with use nonparametric BDS-statistics. It is in-process shown, that, leaning against difference in absolute concepts in a phase space random, regular and random processes with independent values it is possible to solve a problem estimates of parameters representation on observation of random time series against a white noise. Outcomes of numerical modeling of the offered method of an estimate of parameters of random representations for various character of noise are resulted.**
Ключевые слова: **Скрытность, хаотические сигналы, BDS-статистика, оценка параметров.**

Некоторые фундаментальные свойства динамического хаоса вызвали естественный интерес исследователей к их использованию для обеспечения скрытности работы радиосистем (излучаемых ими сигналов) [1]. Достоинства таких радиосистем определяются использованием для передачи сообщений случайно-подобных во временной (спектральной) области хаотических процессов (последовательностей), которые маскируют сигнал под шум. Однако, в отличие от случайных, «малоразмерные» хаотические процессы и последовательности, при их анализе на фазовой плоскости (фазовом пространстве), имеют регулярную структуру и это свойство снижает их скрытность.

В дальнейшем под скрытностью будем понимать [2] способность противостоять мерам радиотехнической разведки: обнаружению сигнала и определению его структуры на основе оценки ряда его параметров без учета возможности раскрытия смысла информации.

Традиционно при оценке вероятности разведки (вероятности обнаружения и раскрытия структуры сигнала) используется энергетический критерий и не учитывается “форма” сигнала. Оптимальный обнаружитель представляет собой измеритель мощности процесса, позволяющий выявлять энергетические приращения над мощностью шумов при наличии сигнала в анализируемом диапазоне частот. В тоже время, понятие “форма” процесса рассматриваемое как лингвистическая характеристика, которая косвенно определяет зависимость его элементов, может быть формализована (представлена численной мерой) и способна дать более объективную оценку вероятности разведки [3]. Такая формализация может быть выполнена, например, с помощью следующей последовательности: “форма” процесса $\rightarrow$ структурированность аттрактора процесса $\rightarrow$ зависимость значений процесса $\rightarrow$ критерий зависимости (динамический или статистический) $\rightarrow$ мера зависимости (например, динамические инварианты: показатели Ляпунова, корреляционная размерность или энтропия). Корреляционной размерностью можно характеризовать структурированность аттрактора (устойчивую упорядоченность его элементов и связей), связанного с анализируемым процессом. Например, случайный I.I.D (independent and identically distributed) процесс неструктурирован, его аттрактор полностью “заполняет” пространство вложения, а

корреляционная размерность совпадает с его размерностью. Особенностью аттрактора хаотического процесса является его структурированность, упорядоченное заполнение" пространства вложения, а также насыщение корреляционной размерности по мере увеличения размерности пространства вложения. Различия в "наполняемости" фазового пространства аттракторами случайного и хаотического процессов и, как следствие, в зависимостях корреляционной размерности и размерности пространства вложения подсказывает один из способов классификации случайных и хаотических процессов, а также решения задачи обнаружения и оценки параметров (раскрытия структуры) хаотических сигналов на фоне шума.

Ниже решим задачу оценки параметров (раскрытия структуры) хаотического отображения по сформированному с его помощью сигналу, наблюдаемому на фоне шума, опираясь на свойства BDS-статистики.

BDS-статистика и построенная на ее основе относительно новая процедура – BDS-тест были предложены в результате анализа финансовых рынков экономистами Броком, Дечертом и Шейнкманом (B. Brock, W. Dechert и J. Scheinkman) в 1987 [3] и представляют один из мощных методов выявления зависимостей во временных рядах, интенсивно разрабатываемых в последнее десятилетие в рамках их нелинейного анализа.

Его цель состоит в том, чтобы различить данные I.I.D. и любой вид зависимости – проверить нулевую гипотезу H_0 о независимости и тождественном распределении значений временного ряда $\vec{x} = (x_1, x_2, ..., x_N)$, используя для этого критерий значимости.

BDS-тест основан на статистической величине $w(\vec{x})$ (BDS-статистике)

$$w_{m,N}(\varepsilon) = \sqrt{N-m+1}\,\frac{C_{m,N}(\varepsilon) - C_{1,N-m}(\varepsilon)^m}{\sigma_{m,N}(\varepsilon)}. \qquad (1)$$

В работе [4] были предложены очень быстрые алгоритмы для её оценки. Числитель BDS-статистики определяется "корреляционными интегралами" $C_{m,N}(\varepsilon)$, $C_{1,N}(\varepsilon)$, а знаменатель среднеквадратическим отклонением $\sigma_{m,N}(\varepsilon)$ числителя. Для вычисления $C_{m,N}(\varepsilon)$ $(m > 1)$ необходимо выполнить «вложение» временного ряда в m-мерное псевдофазовое пространство, элементами которого, на основании теоремы Такенса (Takens) [5], являются точки $x_i^m = (x_i, x_{i+1}, ..., x_{i+m})$ с координатами $\{x_{i+k}\}_{k=1}^m$, заданными m последовательными значениями исходного временного ряда. Корреляционный интеграл определяет частоту попадания произвольной пары точек фазового пространства в гиперсферы радиуса ε:

$$C_{m,N}(\varepsilon) = \frac{2}{(N-m+1)(N-m)} \sum_{s=m}^{N} \sum_{t=s+1}^{N} \prod_{j=0}^{m-1} I_\varepsilon(x_{s-j}^m, x_{t-j}^m),$$

$$I_\varepsilon(x_i^m, x_j^m) = \begin{cases} 1, & \left\| x_i^m - x_j^m \right\| \le \varepsilon \\ 0, & \left\| x_i^m - x_j^m \right\| > \varepsilon \end{cases}, \qquad (2)$$

в котором $I_\varepsilon(x_i^m, x_j^m)$ – функция Хевисайда для всех пар значений i и j, где $0 \le i \le N$ и $0 \le j \le N$; N – число элементов временного ряда $\{x_i\}_{i=1}^N$. Его значение стремится к определенному пределу по мере уменьшения ε. Рекомендуется выбирать ε таким, что $\varepsilon = 0.5\sigma \div 2\sigma$, где σ - среднеквадратическое отклонение процесса $\{x_i\}_{i=1}^N$. В соответствии с теорией, зависимость корреляционного интеграла от ε имеет степенной вид $C_{m,N}(\varepsilon) \sim \varepsilon^{D_c}$, где D_c – корреляционная размерность временного ряда. Для $m = 1$ имеем:

$$C_{1,N}(\varepsilon) = \frac{2}{N(N-1)} \sum_{s=1}^{N} \sum_{t=s+1}^{N} I_\varepsilon(x_s, x_t). \qquad (3)$$

Брок и др. показали, что $C_{m,N}(\varepsilon) \Rightarrow C_{1,N}(\varepsilon)^m$ с 100% вероятностью при $N \to \infty$, а $\left(C_{m,N}(\varepsilon) - (C_{1,N}(\varepsilon))^m\right) \cdot \sqrt{N-m+1}$ является случайной асимптотически нормально распределенной величиной с нулевым средним и среднеквадратическим отклонением $\sigma_{m,N}(\varepsilon)$, которое определяется как:

$$\sigma_{m,N}(\varepsilon) = 2\sqrt{k^m + 2\sum_{j=1}^{m-1} k^{m-j} \cdot (C_{1,N}(\varepsilon))^{2j} + (m-1)^2 \cdot (C_{1,N}(\varepsilon))^{2m} - m^2 k (C_{1,N}(\varepsilon))^{2m-2}}, \quad (4)$$

где $k = \frac{1}{(N-1)(N-2)N}\left\{\sum_{t=1}^{N}\left[\sum_{s=1}^{N} I_\varepsilon(x_t, x_s)\right]^2 - 3\sum_{s=1}^{N}\sum_{t=s+1}^{N} I_\varepsilon(x_t, x_s) + 2N\right\}$.

BDS-статистика $w(\vec{x})$ является нормально распределенной случайной величиной при условии, что оценка $\hat{\sigma}_{m,N}(\varepsilon)$ близка к ее теоретическому значению $\sigma_{m,N}(\varepsilon)$ [6].

Задача обнаружения хаотического сигнала рассматривается как непараметрическая проверка одной из двух гипотез: H_0 – наблюдаемые данные $\vec{x} = (x_1, x_2, ..., x_N)$ независимы и одинаково распределены (белый шум), т. е. плотность (функция) распределения факторизуется $F_N(x_1, x_2, ..., x_N) = \prod_{i=1}^{N} F(x_i)$ и H_1 – данные не I.I.D., что возможно в случае, когда они являются аддитивной смесью шума и сигнала, значения которого зависимы.

В качестве теста на достоверность гипотезы H_0 об отсутствии в наблюдении хаотического процесса принимается выполнение неравенства $|w_{m,N}(\varepsilon)| \le 1{,}96$ для значения статистики $w_{m,N}(\varepsilon)$, что соответствует уровню значимости $\alpha = 0{,}05$ (вероятности ошибки первого рода), тогда с 95% уверенностью можно принять гипотезу H_0 (I.I.D.). Критическая область уровня $\alpha = 0{,}05$, состоит из двух бесконечных полуинтервалов $(-\infty, -1.96]$ и $[1.96, \infty)$. В отсутствие шумов наблюдения применение критерия значимости к статистике $w_{m,N}(\varepsilon)$ позволяет эффективно решать задачу классификации наблюдения ($w_{m,N}(\varepsilon) > |1{,}96|$).

Рассмотрим задачу оценки параметра (раскрытия структуры) логистического отображения по наблюдению:

$$y_n = x_n + \xi_n, \quad (5)$$

где x_n - динамическая переменная (сигнал), заданная одномерным квадратичным отображением $x_{n+1} = 1 - kx_n^2$, $k = k_{ucm}$ - параметр отображения (ключ), ξ_n - последовательность независимых случайных величин, распределенных по нормальному закону с нулевым средним и дисперсией σ_n^2.

Оценка параметра k может быть осуществлена по невязке

$$r_n(\hat{k}) = y_n - s_n(\hat{k}), \quad (6)$$

наблюдения y_n и ожидаемого сигнала $s_{n+1} = 1 - \hat{k}s_n^2$ с предполагаемым значением параметра $\hat{k}$.

При совпадении оцениваемого параметра с истинным значением $\hat{k} = k_{ucm}$, имеем $s_n(\hat{k}) = x_n$ и, следовательно $r_n(\hat{k}) = \xi_n$. Тогда BDS-статистика (1) от разности $\{r_n(\hat{k}) = \xi_n\}_{n=1}^{N}$ с 95% вероятностью позволяет принять гипотезу H_0 (невязка представляет последовательность I.I.D.). Другими словами значения BDS-статистики будут минимальны и попадать в доверительный интервал $[-1{,}96; 1{,}96]$.

На рис. 1 проиллюстрирована процедура формирования невязки. При совпадении оцениваемого параметра с истинным значением фазовый портрет разностного сигнала повторяет фазовый портрет белого гауссовского шума.

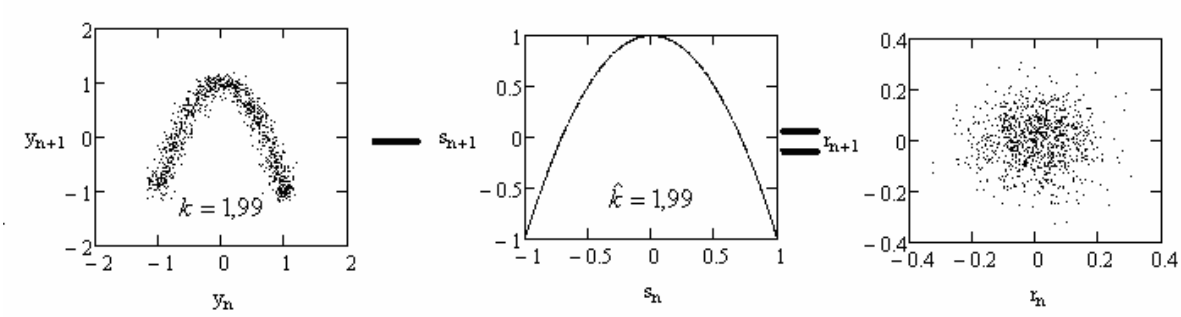

Рисунок 1 – Формирование фазового портрета разности наблюдаемой и ожидаемой последовательностей при $\hat{k} = k_{ucm}$

Очевидно, что рассогласование между параметрами $\hat{k} \neq k_{ucm}$ будет приводить к наличию в невязке двух хаотических последовательностей и шума. Её аттрактор проявляет структурированность (см. рис. 2) и, как следствие, увеличение значения BDS-статистики $\left|w_{m,N}\left(\hat{k}\right)\right| > 1{,}96$.

В качестве BDS-оценки параметра k примем его значение, минимизирующее функцию (1):

$$\hat{k}_{BDS} = \min_{k}\left[\overline{w}_{m,N}(k)\right]. \qquad (7)$$

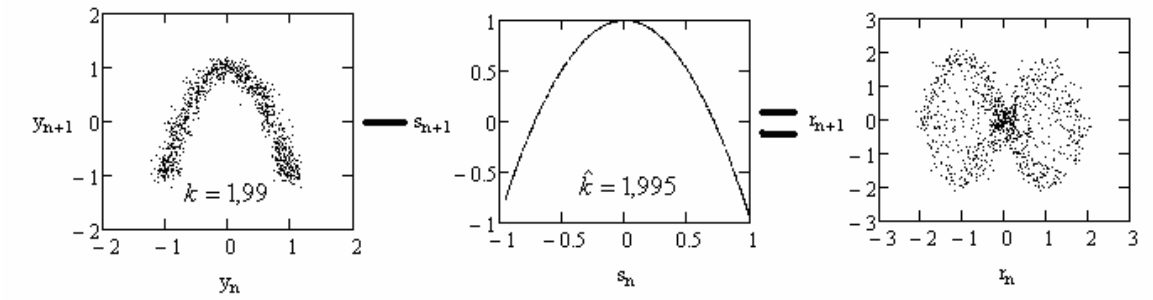

Рисунок 2 – Формирование фазового портрета разности наблюдаемой и ожидаемой последовательностей при $\hat{k} \neq k_{ucm}$

На рис. 3 приведены результаты численного моделирования зависимости среднего значения BDS-статистики $\overline{w}_{m,N}\left(\hat{k}\right)$, полученного для пяти реализаций шума при $x_0 = 0{,}216$, $k_{ucm} = 1{,}99$, $N = 1000$. Непрерывной кривой показана зависимость BDS-статистики от оцениваемого параметра в отсутствие шума, $\sigma_n^2 = 0$, а пунктирной – при наличии гауссовского шума для отношения сигнал/шум по мощности $q^2 = \sigma_x^2 / \sigma_n^2 = 10$. Точками, обозначена кривая, полученная при наличии в аддитивной смеси шума с равномерным распределением. Из рисунка видно, что для выбранных значений q^2 все зависимости имеют выраженные минимумы. В отсутствии шума минимум зависимости $\overline{w}_{m,N}(k)$ располагается вблизи истинного значения оцениваемого параметра, т. е. $\hat{k} \approx k_{ucm}$. Увеличение уровня шума уменьшает крутизну зависимости $\overline{w}_{m,N}(k)$ в окрестности истинного значения параметра $k_{\text{èñò}}$, расширяет и смещает относительно истинного значения интервал его возможных значений при заданном уровне значимости.

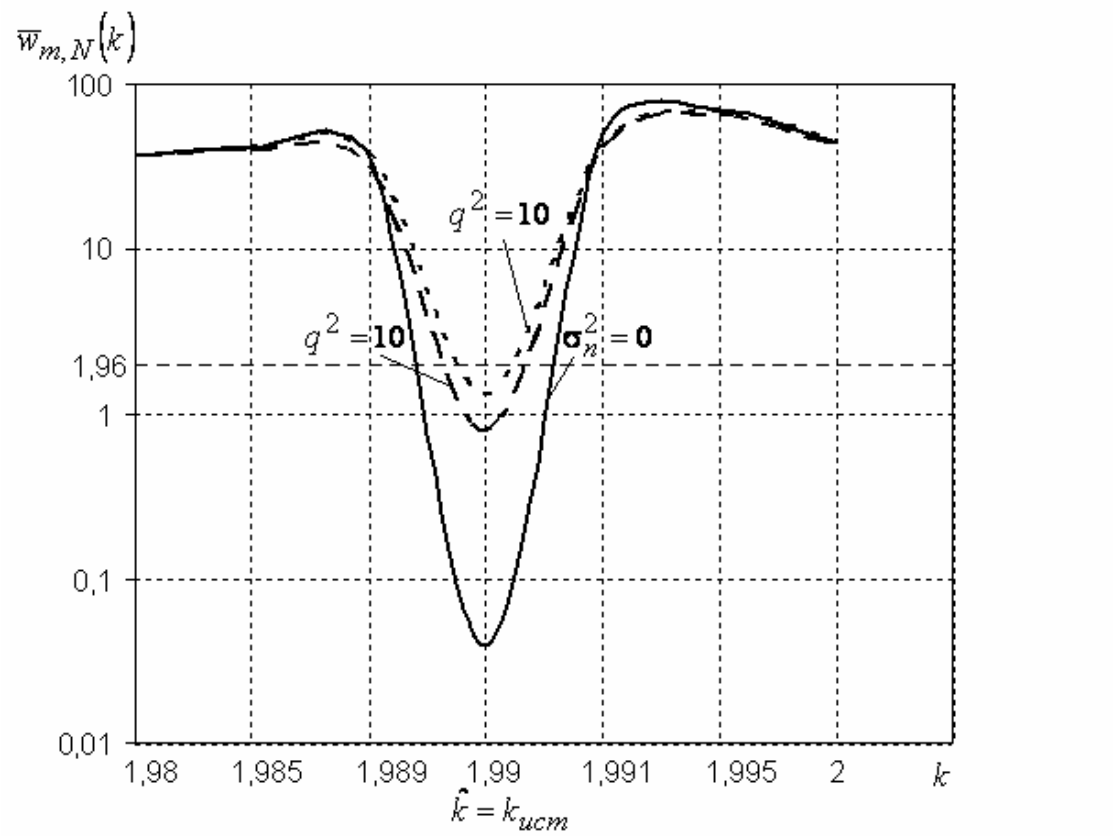

Рисунок 3 – Зависимость BDS-статистики от изменения значений оцениваемого параметра $\hat{k}$

Предложенный в работе метод, основанный на применении непараметрической BDS-статистики, позволяет с заданной вероятностью давать интервальную и точечную оценку параметра одномерного отображения по наблюдению хаотического временного ряда на фоне аддитивного шума. Полученные результаты, в отличие от известных подходов к оценке разведзащищенности информационных систем, основанных на применении энергетических признаков сигналов и помех, могут быть использованы для более объективной оценки скрытности хаотических и шумоподобных сигналов.

Литература: ***1.*** *Дмитриев А. С. Динамический хаос как парадигма современных систем связи/ А. С. Дмитриев, А. И. Панас, С. О. Старков// Зарубежная радиоэлектроника, – 1997, №10, – С. 4-26.* ***2.*** *Тузов Г. И. Помехозащищенность радиосистем со сложными сигналами / Г. И. Тузов, В. А. Сивов, В. И. Прытков и др. // М.: Радио и связь. – 1985. – 264 с.* ***3.*** *Васюта К. С. Обнаружение хаотического процесса искаженного белым шумом с использованием BDS- статистики/ Костенко П. Ю., Барсуков А. Н., Симоненко С. Н. //Из. ВУЗ Радиоэлектроника. –Киев: 2009. – Том. № 52.- № 11.- с 41-51.* ***4.*** *Kanzler Ludwig Very Fast and Correctly Sized Estimation of the BDS Statistic / Ludwig Kanzler // Christ Church and Department of Economics University of Oxford. – 1999. – 95 P.* ***5.*** *Holger Kantz Nonlinear time series analysis/ Holger Kantz and Thomas Schreiber // Second edition Printed in the United Kingdom at the University Press, Cambridge – 2004. – 369 P.* ***6.*** *Brock W. A. A Test of Nonlinear Dynamics, Chaos, and Instability / Brock W. A., D. Hsieh, and B. LeBaron // Cambridge: MIT Press. – 1991.*