УДК 621.34

С.Г. Семенов, Т.С. Резниченко, Д.Ю. Задорожний

Национальный технический университет «ХПИ», Харьков

УСОВЕРШЕНСТВОВАННЫЙ МЕТОД СТРУКТУРНОЙ ИДЕНТИФИКАЦИИ КОМПЬЮТЕРНЫХ СИСТЕМ КРИТИЧЕСКОГО ПРИМЕНЕНИЯ

Проведен анализ метода идентификации трафика на основе BDS-тестирования. Выявлены характерные его недостатки и предложены пути их устранения. Определены структуры динамических подсистем в компьютерных системах критического применения. Разработан алгоритм формирования «квазициклов». Усовершенствованный метод структурной идентификации компьютерной системы критического применения на основе комплексного использования наблюдаемого структурно-информационного портрета и BDS-теста.

Ключевые слова: *компьютерные системы критического применения, структурная идентификация, BDS-тест, наблюдаемый структурно-информационный портрет.*

Введение

Постановка проблемы. В процессе исследования сложных систем методами нелинейной динамики одним из приоритетных вопросов остается вопрос определения структуры объектов управления (структурной идентификации). До недавнего времени большинство методов структурной идентификации строились на основе центральной предельной теоремы и предположении о том, что изучаемая система является или случайной или детерминированной. Однако, как показали исследования ряда авторов [3 – 9], существуют системы, в которых протекающие процессы обладают одновременно свойствами случайности и детерминизма.

При определенных условиях (использование гетерогенных сетевых технологий, циркуляция мультисервисного трафика, применение современных протоколов и средств защиты информации на разных уровнях модели *NGN* и др.) эта особенность наблюдается и в компьютерных системах критического применения (КСКП). Поэтому решение вопроса структурной идентификации КСКП во многом связано с определением «формы» входных и выходных данных.

Анализ литературы [3 – 9] показал, что одним из направлений решения указанной задачи является структурная идентификация на основе BDS-тестирования. Проведенные исследования метода структурной идентификации КСКП на основе BDS-теста, а также анализ процесса выявления статистических зависимостей в состоянии КСКП в условиях внешних воздействий показал ряд характерных недостатков, присущих данному методу. В первую очередь это его высокая вычислительная сложность. Так, например, статистическая выборка размером 1000 отсчетов, обрабатываемая на персональном компьютере, основные характеристики которого представлены на рис. 1 требует временных затрат в размере $T_{BDS} \approx 40$ с, а выборки в 5000 T_{BDS} уже превышает 3 минуты, что недопустимо для систем идентификации в режиме реального времени.

Поле	Значение
Компьютер	
Тип компьютера	ACPI x64-based PC
Операционная система	Microsoft Windows 7 Enterprise
Пакет обновления ОС	Service Pack 1
Internet Explorer	9.0.8112.16421
DirectX	DirectX 11.0
Имя компьютера	SERGEY-PC
Имя пользователя	Sergey
Вход в домен	Sergey-PC
Дата / Время	2013-04-05 / 09:28
Системная плата	
Тип ЦП	TripleCore , 2300 MHz (11.5 x 200)
Системная плата	Lenovo Guam
Чипсет системной платы	AMD 760G/780G/780V/785G/790GX, AMD K10
Системная память	3066 Мб (DDR3 SDRAM)
Тип BIOS	Insyde (05/25/11)

Рис. 1. Основные характеристики компьютера, используемого для проведения экспериментов

Устранить указанный недостаток предлагается путем определения структуры динамических подсистем КСКП и использования в качестве статистических данных анализа состояния системы координат особых точек наблюдаемых структурно-информационных портретов (центров квазициклов аттрактора).

Основная часть

1. **Определение структуры динамических подсистем в КСКП.** Проведенные анализ и исследования КСКП показали целесообразность использования фазовых и наблюдаемых структурно-информационных портретов в процессе структурной идентификации отдельных динамических подсистем КСКП, а также возможность получения с их помощью определенных заключений о свойствах системы. Однако получение полной информации о состоянии КСКП и ее оценка невозможны без выявления особых точек (корней) динамической системы. Анализ ряда работ [1, 2] показал, что данную задачу чаще всего решают с помощью индексов особых точек.

Пусть z – векторное поле, заданное на ориентированной евклидовой плоскости $\hat{Z}$, порожденное динамической системой. В большинстве практических случаев полю z на евклидовой плоскости $\hat{Z}$ соответствует набор замкнутых кривых $Z_{\text{нсип}}$ ($Z_{\text{lнсип}}$) (фазовый портрет) или Z_i (Z_{li}) (наблюдаемый структурно-информационный портрет). Тогда индексом $\text{ind}(z, Z_{\text{нсип}})$ можно назвать деленную на 2π вариацию поля z вдоль кривых $Z_{\text{нсип}}\langle Z_{\text{lнсип}}, Z_i, Z_{li}\rangle$. Если обозначить, через $D \subseteq \hat{Z}$ область плоскости $\hat{Z}$ с координатами (x_1, x_2), и $\hat{S}$ – как окружность на плоскости $\hat{Z}$, при этом задать отображение области $\hat{D} = D/D_0$ на окружность $\hat{S}$:

$$Z_{\text{нсип}} : \hat{D} \to \hat{S},\ Z_{\text{нсип}}(X) = F(X)/\|F(X)\|, \quad X \in R2,$$

$$\langle Z_{\text{lнсип}}, Z_i, Z_{li}\rangle : \hat{D} \to \hat{S},\ \langle Z_{\text{lнсип}}, Z_i, Z_{li}\rangle(X) = F(X)/\|F(X)\|, \quad X \in R2,$$

где D_0 – область с особыми точками поля, $\|\bullet\|$ – евклидова норма.

Из [2, 3] известно, что индексом ориентированной замкнутой кривой $Z_{\text{нсип}}\langle Z_{\text{lнсип}}, Z_i, Z_{li}\rangle : \hat{D} \to \hat{S}$ называется интеграл от

$$d\phi = d\ \text{arctg}\frac{f_1}{f_2} = \frac{f_2 df_1 - f_1 df_2}{f_1^2 + f_2^2}, \quad f_i(X) \in F(X)$$

по кривой $Z_{\text{нсип}}\langle Z_{\text{lнсип}}, Z_i, Z_{li}\rangle$, деленный на 2π:

$$\text{ind}(Z_{\text{нсип}}\langle Z_{\text{lнсип}}, Z_i, Z_{li}\rangle) = \oint_{Z_{\text{нсип}}} d\phi \Big/ 2\pi.$$

Таким образом, индекс связан только с замкнутыми кривыми $Z_{\text{нсип}}\langle Z_{\text{lнсип}}, Z_i, Z_{li}\rangle$.

Исходя из свойств индекса кривой (неизменности индекса до прохождения через особые точки при деформации замкнутой кривой и векторного поля) указанных в [1,2], можно сделать следующие заключения:

Заключение 1. Если $Z_{\text{нсип}}\langle Z_{\text{lнсип}}, Z_i, Z_{li}\rangle$ состоит из нескольких кривых $z_1, z_2, ...$, то индекс $\text{ind}(Z_{\text{нсип}}\langle Z_{\text{lнсип}}, Z_i, Z_{li}\rangle) = \sum_i \text{ind}(z_i)$.

Заключение 2. Если на некоторой кривой $Z_{\text{нсип}}\langle Z_{\text{lнсип}}, Z_i, Z_{li}\rangle$, ограничивающей область D нет особых точек, а в области D имеется конечное количество особых точек, то индекс кривой $Z_{\text{нсип}}\langle Z_{\text{lнсип}}, Z_i, Z_{li}\rangle$ равен сумме индексов особых точек поля, лежащих внутри.

Заключение 3. Если индекс $Z_{\text{нсип}}\langle Z_{\text{lнсип}}, Z_i, Z_{li}\rangle$ отличен от нуля, то внутри области D, ограниченной кривой $Z_{\text{нсип}}\langle Z_{\text{lнсип}}, Z_i, Z_{li}\rangle$ есть хотя бы одна особая точка.

Используем рассмотренные теоретические положения для реализации усовершенствованного метода структурной идентификации на основе BDS-тестирования.

2. Усовершенствованный метод структурной идентификации КСКП на основе комплексного использования наблюдаемого структурно-информационного портрета и BDS-теста. Для решения поставленной задачи предлагается использовать алгоритм формирования квазициклов, структурная схема которого представлена на рис. 2.

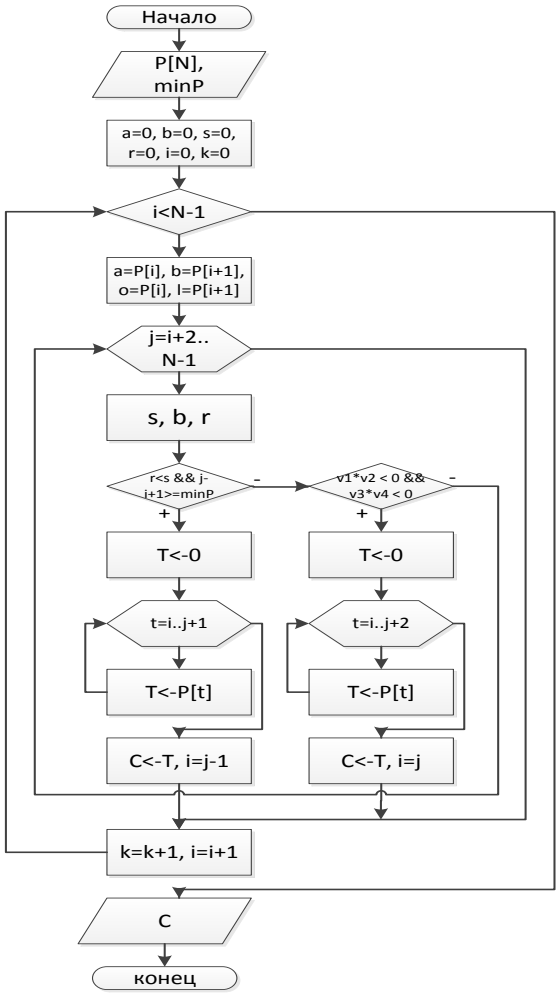


Рис. 2. Схема алгоритма формирования «квазициклов»

Введем следующие обозначения и ограничения:

a – начальная точка «квазицикла»; *b* – текущая точка «квазицикла»; *s* – расстояние от начальной точки «квазицикла» до текущей; d – точка «квазицикла», следующая за точкой *a;* r – расстояние от *a* до d ; i – переменная, характеризующая количество текущих точек в «квазицикле»; *k* – переменная, характеризующая количество «квазициклов»; *C* – множество всех «квазициклов».

Входными данными алгоритма являются: координаты исследуемых характеристик на наблюдаемом структурно-информационном портрете (НСИП), представленными в виде массива $W[N]$, где N – количество точек изменения траектории НСИП; W_{min} – значение минимального количества точек в «квазицикле».

На выходе алгоритма мы должны получить множество «квазициклов», и координат точек изменения траектории НСИП «квазицикла». Целью рассматриваемого алгоритма является определение расстояния s от начальной точки предположительного «квазицикла» a до текущей точки b и расстояния r от точки a до точки d . Пусть «квазицикл» считается найденным, при выполнении следующих условий:

1) $r < s$, $W[N] \geq W_{min}$;

2) отрезок $[o, l]$ пересекается с $[n, m]$.

Каждая точка представлена в виде структуры, содержащей информацию о координатах (x, y).

На первом шаге в цикле по всем точкам НСИП от $i = 0$ по $N-1$, начальной точке a и точке o присваивается значение $P[i](a = o = P[i])$. Точке b и второй точке предполагаемого «квазицикла» l присваивается значение $P[i+1](b = l = P[i+1])$.

На втором шаге в цикле от $j = i+2$ по $N+1$, определяется расстояние s :

$$s = \sqrt{(b.x - a.x)^2 + (b.y - a.y)^2}, \qquad (1),$$

где $i+2$ –индекс 3-й точки предполагаемого «квазицикла».

Изменяя значение текущей точки b (присвоив ей значение $P[j]$) в соответствии с выражением 1 определяется расстояние r . Текущей точке n присваивается значение $P[j]$, а следующей за текущей m – значение $P[j+1]$.

На третьем шаге в соответствии с правилами:

$$v1 = (m.x - n.x)\cdot(o.y - n.y) - (m.y - n.y)\cdot(o.x - n.x);$$

$$v2 = (m.x - n.x)\cdot(l.y - n.y) - (m.y - n.y)\cdot(l.x - n.x);$$

$$v3 = (l.x - o.x)\cdot(n.y - o.y) - (l.y - o.y)\cdot(n.x - o.x),$$

определяется условие пересечения $[0,1]$ и $[n, m]$.

Далее проверяется условие:

$$r < s \vee j - i + 1 \geq \min P. \qquad (2),$$

Если условие 2 выполняется, то формируется множество V координат точек НСИП от i по $j+1$.

На следующем шаге формируется множество C «квазициклов». После этого переменной i присваивается значение $j-1$, чтобы текущая точка стала начальной следующего «квазицикла». На следующих шагах вызывается процедура инкрементации i и происходит возврат к началу алгоритма. При проверке условия 2 определяется возможность окончания алгоритма. В случае если оно не выполнено, то осуществляется проверка условия пересечения отрезков. Если $(v1 \cdot v2 < 0) \vee (v3 \cdot v4 < 0)$, то выполняются все шаги, соответствующие условию 2, с одним изменением – диапазон добавляемых точек формируется в пределах от i до $j+2$ ($i = j$). Далее инкрементируем значение i и возвращаемся на первый шаг.

В целях визуализации на рис. 3 иллюстрируется графическое представление НСИП КСКП на примере злоумышленного потока данных (*Dos*-атаки).

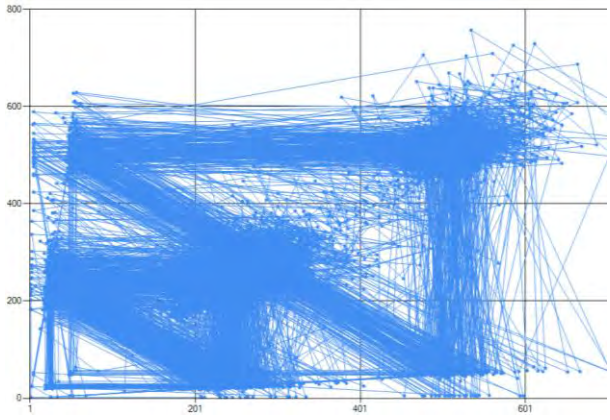
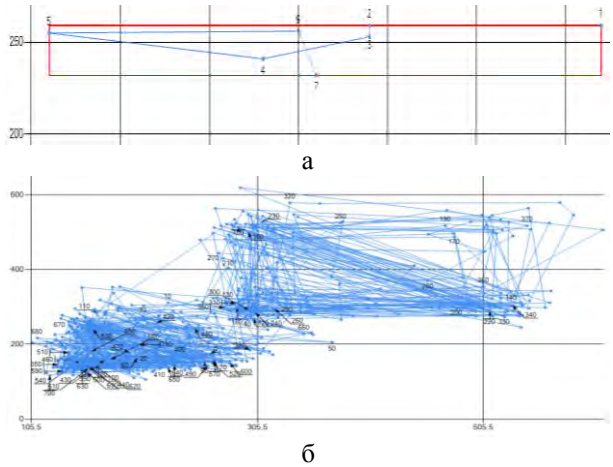


Рис. 3 Графическое представление НСИП КСКП

Рассмотренное разложение двумерного НСИП КСКП портрета на квазициклы в существенной мере базируется на визуализации графического представления (на экране дисплея) фрагментов данного НСИП. При этом принимается во внимание характер вращения звеньев, соединяющих соседние точки (x_i, x_{i+1}), (x_{i+1}, x_{i+2}) визуализируемого фрагмента рассматриваемого НСИП. На рис. 4 в качестве примера представлен первый «квазицикл», с зафиксированными границами (рис. 4 а), а также траектория движения особых (центральных) точек «квазициклов» в НСИП (рис. 4, б). Координаты особых точек используются в качестве входных данных BDS-теста.



а

б

Рис. 4. Изображение» квазицикла» с зафиксированными границами и траектория движения особых (центральных) точек «квазициклов» в НСИП КСКП

Результаты BDS-теста особых точек «квазициклов» представлены в табл. 1. Проведенный анализ результатов тестирования показал, четкую тенденцию снижения значений BDS-статистики в условиях внешних воздействий и непротиворечие полученных результатов оценки статистических особенностей траектории особых точек с результатами BDS-теста полной статистической выборки показателей КСКП.

Таблица 1

Значение *BDS*- статистики особых точек «квазициклов» НСИП КСКП в условиях внешнего воздействия (*Dos*-атаки)

	m=6		m=5		m=4	
	ε=0.5	ε=0.25	ε=0.5	ε=0.25	ε=0.5	ε=0.25
Dos-атака	0.981	2.122	0.993	1.997	1.003	3.192

Выводы

Таким образом, в ходе исследования определено, что для идентификации КСКП и определения аномального поведения в ряде практических случаев целесообразно использовать *BDS*-тестирование.

Для уменьшения времени тестирования усовершенствован метод структурной идентификации КСКП на основе *BDS*-тестирования, учитывающий статистические зависимости в изменениях состояния системы в условиях внешних воздействий, что позволяет уменьшить время структурной идентификации системы до 2 раз. по сравнению с используемыми в компьютерных системах стандартными средствами идентификации.

Список литературы

1. *Карабутов Н.Н. Адаптивная идентификация систем: Информационный синтез / Н.Н. Карабутов. – М.: КомКнига, 2006. – 384 с.*
2. *Карабутов Н.Н. Структурная идентификация систем: анализ динамических структур / Н.Н.Карабутов. – М.: МГИУ, 2008. – 160 с.*
3. *Костенко П.Ю. Обнаружение хаотического процесса искаженного белым шумом с использованием BDS-статистик / П.Ю. Косенко, А.Н. Барсуков, К.С. Васюта, С.Н. Симоненко // Радиоэлектроника. – 2009. – Т. 52, № 11. – С .41-50 – (Изв. вузов).*
4. *Кузнецов О.О. Метод структурной идентификации информационных потоков в телекоммуникационных сетях на основе BDS-тестирования / О.О. Кузнецов, С.Г. Семенов, С.Н. Симоненко, Е.В. Мелешко // Наука і техніка Повітряних Сил Збройних Сил України: науково-технічний журнал. –2010. – № 2 (4). – С.131-136.*
5. *Семенов А.Д. Идентификация объектов управления: уч. пос. / А.Д. Семенов, Д.В. Артамонов, А.В. Брюхачев. – Пенза: Изд-во Пенз. гос. ун-та, 2003. – 211 с.*
6. *Семенов С.Г. Структурно-информационный портрет информационной системы в условиях неопределенности на примере Dos-атаки / С.Г. Семенов // Радиотехника. Информационная безопасность. – Х.: ХНУРЕ, 2011. – №166. – С. 99-106.*
7. *Brock W. A test for independence based on the correlation dimension / W. Brock. W. Dechert, J. Scheinkman // Working Paper, University of Wisconsin, 1987.*
8. *W. Brock D. Hsieh and B. LeBaron. "Non-linear Dynamics, Chaos, and Instability", Cambridge, Massachusetts: The MIT Press, USA, 1991.*
9. *W. Brock, W. Dechert, J. Scheinkman and B. LeBaron. "A test for independence based on correlation dimension", Econometric Reviews 15: 197-235, 1996.*

Поступила в редколлегию 24.10.2012

Рецензент: д-р техн. наук, проф. В.А. Краснобаев, Полтавский национальный технический университет им. Ю. Кондратюка, Полтава.

ВДОСКОНАЛЕНИЙ МЕТОД СТРУКТУРНОЇ ІДЕНТИФІКАЦІЇ КОМП'ЮТЕРНИХ СИСТЕМ КРИТИЧНОГО ЗАСТОСУВАННЯ

С.Г. Семенов, Т.С. Резніченко, Д.Ю. Задорожній

Проведений аналіз методу ідентифікації трафіка на основі BDS-тестування. Виявлені характерні його недоліки і запропоновані шляхи їх усунення. Визначені структури динамічних підсистем в комп'ютерних системах критичного застосування. Розроблений алгоритм формування «квазіциклів». Вдосконалений метод структурної ідентифікації комп'ютерної системи критичного застосування на основі комплексного використання спостережуваного структурно-інформаційного портрета і BDS-теста.

Ключові слова: *комп'ютерні системи критичного застосування, структурна ідентифікація, BDS-тест, спостережуваний структурно-інформаційний портрет.*

IMPROVED METHOD OF STRUCTURAL AUTHENTICATION OF COMPUTER SYSTEMS OF CRITICAL APPLICATION

S.G. Semenov, T.S. Reznichenko, D.Yu. Zadorozhniy

The analysis of method of authentication of traffic is conducted on the basis of BDS-test. His characteristic failings are exposed and the ways of their removal are offered. The structures of dynamic subsystems are certain in the computer systems of critical application. The algorithm of forming of cycles is developed. Improved method of structural authentication of the computer system of critical application on the basis of the complex use of the looked after portrait and BDS-test.

Keywords: *computer systems of critical application, structural authentication, BDS-test, looked after portrait.*