АНАЛИЗ МЕТОДА ОБНАРУЖЕНИЯ СЕТЕВЫХ АНОМАЛЬНЫХ ВЫБРОСОВ ТРАФИКА С ПОМОЩЬЮ АЛГОРИТМА БРОДСКОГО-ДАРХОВСКОГО

Скибин В.П., Поповский В.В.

Харьковский национальный университет радиоэлектроники, Украина.

E-mail: vladislav.skibin@gmail.com

Abstract

In this paper we are considering algorithms of detection of network anomaly burst with method of disorder by Brodsky-Darkhovsky. As a processed statistic we are used Brodsky-Darkhovsky's generalized statistic, used for the test of mach/mismatch for the mean value in two sliding windows/. Conducted simulations of attacks on telecommunication system and their detection using this algorithm. Identified the critical values of noise for normal mode and the sliding window in which the algorithm ceases to function properly. The practical examples with a clear illustration of the algorithm is applied.

Используемый метод

Системы обнаружения сетевых вторжений и выявления признаков атак на информационные системы сегодня широко применяются как один из необходимых рубежей обороны информационных систем. В связи с этим актуальность приобретает задача скорейшего обнаружения момента изменения вероятностных характеристик случайной последовательности работы сети (момента «разладки»). Представляет интерес возможность применения теории обнаружения разладки в задаче обнаружения аномальных выбросов трафика в сети, вызванных различными компьютерными атаками и вредоносным воздействием вирусов.

В работах [1, 2] авторами был предложен метод обнаружения разладки, основанный на обнаружении изменения среднего значения случайного процесса. Данный метод является непараметрическим. Преимуществами подобных методов является их независимость от распределений, отсутствие необходимости наличия априорных данных и возможность организовывать корреляционный ряд из выборочных значений.

Пусть $X = \{x(n)\}_{n=1}^{N}$ - случайный процесс с дискретным временем, причем известно, что случайные величины $x(1), x(2), ... x(n)$ имеют общую одномерную функцию распределения. Требуется по наблюденной реализации процесса X определить моменты начала и окончания разладки.

В общем виде алгоритм Бродского-Дарховского выглядит следующим образом:

$$Y(n) = \left[\frac{n}{N}\left(1-\frac{n}{N}\right)\right]^{v}\left(\frac{1}{n}\sum_{1}^{n}x_i - \frac{1}{N-n}\sum_{n+1}^{N}x_i\right), \quad (1)$$

$$\hat{n}_0 = \mathbf{max}|Y(n)|, \quad (2)$$

где n – шаг, на котором производится оценка, $\hat{n}_0$ - оценка момента возникновения аномалии. [3]

В случае, когда обнаружение разладки производится в реальном времени методом скользящего окна размера m, смещающегося слева направо по мере поступления данных алгоритм приобретает вид:

$$Y(m) = \left[\frac{n}{N}\left(1-\frac{n}{N}\right)\right]^{v}\left(\frac{1}{n}\sum_{1}^{n}x_{i,m} - \frac{1}{N-n}\sum_{n+1}^{N}x_{i,m}\right), \quad (3)$$

$$\hat{n}_0 = \max\left|Y(m)\right|, \tag{4}$$

где m – размер скользящего окна.

В отличии от алгоритма [1] решение о наличии аномального выброса принимается не во всей реализации, а в каждом конкретном окне. Данная схема позволяет динамически отслеживать изменения в сети и быстрее реагировать на них.

Анализ работы алгоритма Бродского-Дарховского в обычном режиме

В алгоритме Бродского-Дарховского [1] присутствует некий коэффициент $\left[\frac{n}{N}\left(1-\frac{n}{N}\right)\right]^v$ (3), который зависит от шага наблюдения и степени v, значение которого влияет непосредственно на выход $Y(n)$. Была проанализирована зависимость изменения данного коэффициента от шага наблюдение при различных значениях v, так как такого рода исследование не было проведено в работе [3]. Результаты приведены на рис. 1.

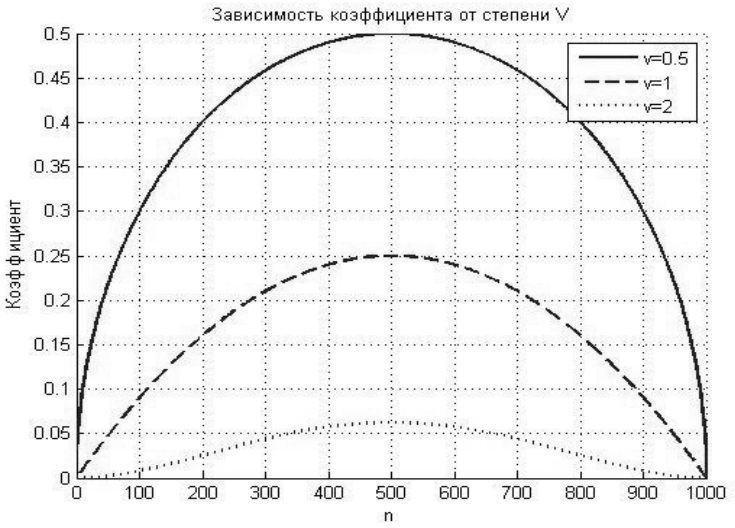

Рис.1. Зависимость коэффициента от шага обнаружения и *v*

Анализируя график можно сделать вывод, что путем изменения v можно адаптировать алгоритм для систем с различным уровнем стабильности работы (чем стабильнее система – тем ниже v). Кроме того данный коэффициент снижает доверие к значениям $Y(n)$, полученным в начальных и конечных значениях интервалах n и повышает доверие в момент накопления статистики (середина интервала).

На рис. 2 и рис. 3 представлены результаты моделирования работы алгоритма Бродского-Дарховского при имитации аномального воздействия на определенном интервале при различном уровне шума. Как видно из графиков, алгоритм четко определяет момент начала и конца разладки при отсутствии шума и уровне шума, равном уровню сигналу. При превышении значения шума над значение сигнала в 2 и более раз алгоритм работает нестабильно и появляется вероятность появления ошибок первого и второго рода.

Анализ работы алгоритма Бродского-Дарховского в режиме скользящего окна

При использовании скользящего окна для обнаружения разладки методом Бродского-Дарховского [3] были проведены исследования качества обнаружения аномалий от размера окна и уровня шума. Исходя из результатов исследования, можно сделать вывод, что размер окна может варьироваться в применимых для данной системы пределах, он может как быть меньше промежутка

выброса, так и превышать его. Алгоритм в режиме скользящего окна позволяет обнаружить выброс при значительном уровне шумов, в том числе и превышении шумами уровня сигнала. Некоторые из результатов работы системы в данном режиме приведены на рис.4 и рис.5.

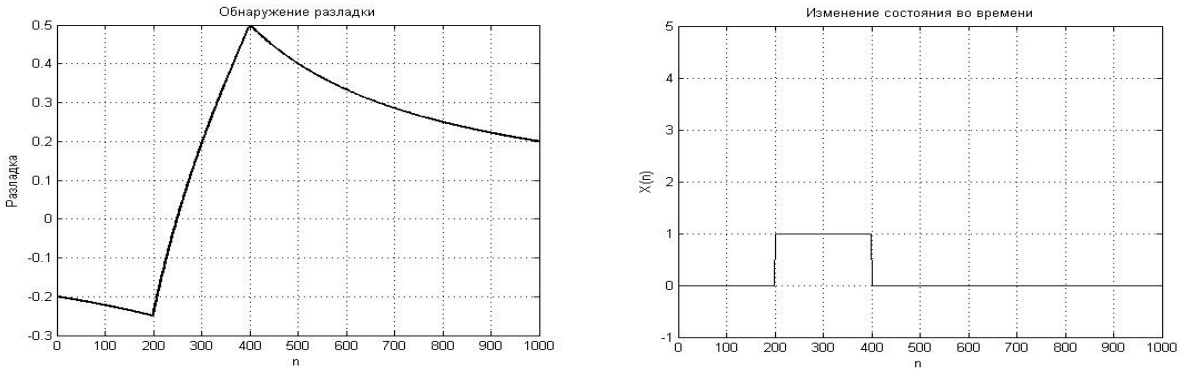

Рис.2. Обнаружение аномального выброса при нулевом уровне шума

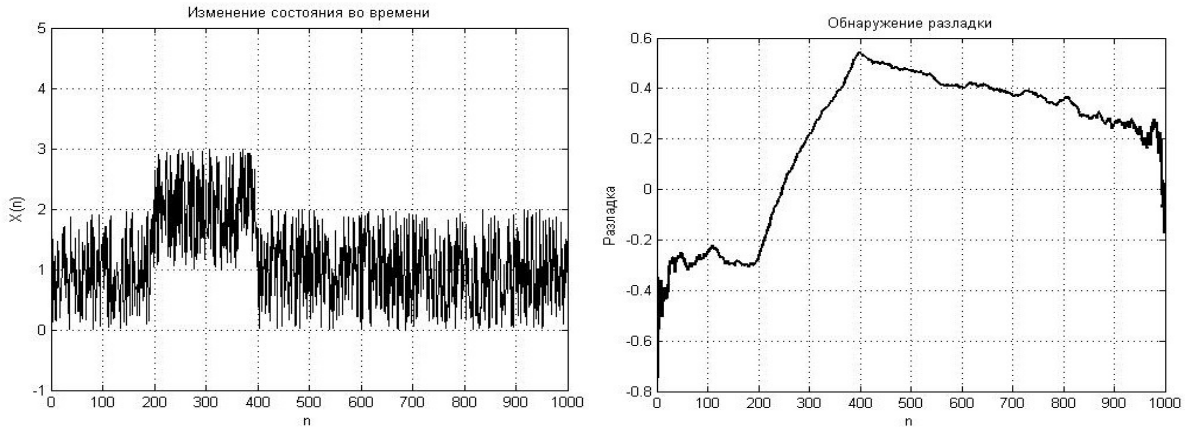

Рис.3. Обнаружение аномального выброса при SNR=1/2

Как видно на рис. 4 и рис. 5 при использовании алгоритма Бродского-Дарховского в этом режиме в начале и конце атаки наблюдаются максимальные значения решающей статистики, которые позволяют зафиксировать начало и конец атаки, характеризующейся измерением среднего значения трафика. Результатом работы данного алгоритма является решение о наличии или отсутствии аномалии на каждом из шагов.

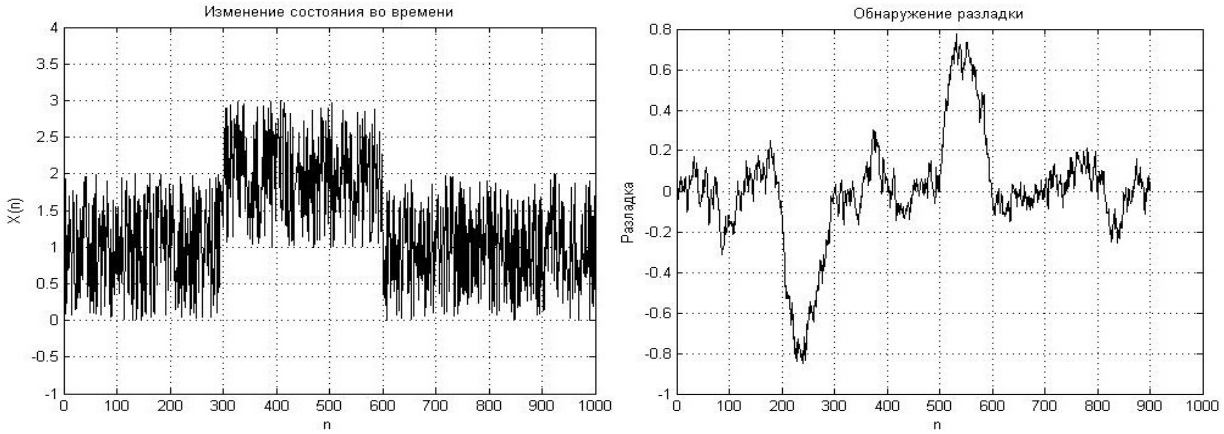

Рис.4. Обнаружение выброса окном равном 100 и SNR=1/2

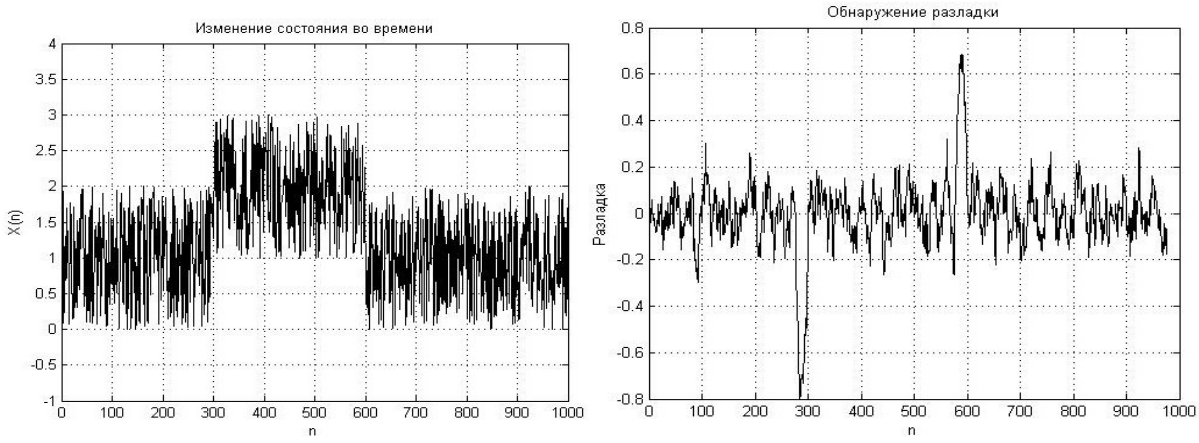

Рис.5. Обнаружение выброса окном равном 25 и SNR=1/1

Выводы

Для обнаружения аномальных выбросов трафика предложено использовать алгоритм Бродского-Дарховского в стандартном режиме и режиме скользящего окна. Проведено имитационное моделирование атак на телекоммуникационную систему и их обнаружения при помощи данного алгоритма. Сделан вывод, что при выборе традиционного алгоритма (1) особое влияние проявляют шумы. Так сравнение рис. 2 и рис.3, на которых изображены реакции процедуры на разладку в отсутствии шумов (рис. 2) и присутствии шумов (рис.3), показывает, что обнаружение во втором случае становится проблематичным. При выборе алгоритма в режиме скользящего окна совокупное действие помех уменьшается, и выбросы, характеризующие начало и конец воздействия, представляются в более явном виде (рис. 4 и рис. 5).

В работе показано, что для практической реализации лучше использовать алгоритм в режиме скользящего окна, доказана его эффективность. Приведены практические примеры с наглядной иллюстрацией работы алгоритма.

Литература:

1. *Дарховский Б.С, Бродский Б.Е.* Апостериорное обнаружение момента «разладки» случайной последовательности. // Теория вероятностей и ее применение. – 1980. – Т. 25, № 3 – С. 635-639.

2. *Бродский Б.Е*, *Дарховский Б.С.* Асимптотический анализ некоторых оценок в апостериорной задаче о разладке // Теория вероятностей и ее применения. – 1990. – Т. 35, № 3. – С. 551-557.

3. *Шелухин О.И.*, *Филиппова А.С.* Обнаружение сетевых аномальных выбросов трафика методом разладки // Труды СКФ МТУСИ, 2013. – С. 245-248.