INTRUSION DETECTION METHOD ACCORDING TO THE CHARACTERISTICS OF REFRESHING PROCESS

Snegurov A.V., Skibin V.P., Chakryan V.H.
Kharkiv National University of Radioelectronics
Department of Telecommunication Systems
14, Lenin Ave., Kharkiv, 61166, Ukraine
Ph.: (057) 7021320, e-mail: vladislav.skibin@gmail.com

Abstract — The method of intrusions detecting in telecommunication systems by analyzing the characteristics of a number of values of innovation process is proposed. The hypothesis notifies that in the absence of anomalous effects of the discrepancy corresponds to the parameters of the Gaussian white noise is considered. As a criterion to determine the correlation residuals and the Gaussian white noise we propose to use the Wilcoxon signed rank test. The reason of a choice of this criterion is also considered.

МЕТОД ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ ПО ХАРАКТЕРИСТИКАМ ОБНОВЛЯЮЩЕГО ПРОЦЕССА

Снегуров А. В., Скибин В. П., Чакрян В. Х.
Харьковский национальный университет радиоэлектроники
каф. Телекоммуникационных систем
пр. Ленина, 14, Харьков, 61166, Украина
тел.: (057) 7021320, e-mail: vladislav.skibin@gmail.com

Аннотация — В работе предложен метод обнаружения вторжений в телекоммуникационные системы путем анализа характеристик ряда значений обновляющего процесса. Рассматривается гипотеза, что в отсутствии аномального воздействия невязка соответствует параметрам гауссового белого шума. В качестве критерия для определения корреляции невязки и гауссового белого шума в работе предлагается использовать ранговый критерий Уилкоксона. Приведены обоснования выбора именно этого критерия.

I. Введение

Системы обнаружения сетевых вторжений и выявления признаков атак на информационные системы уже давно применяются как один из необходимых рубежей обороны информационных систем. На сегодня системы обнаружения вторжений и атак обычно представляют собой программные или аппаратно-программные решения, которые автоматизируют процесс контроля событий, протекающих в компьютерной системе или сети, а также самостоятельно анализируют эти события в поисках признаков проблем безопасности. Поскольку количество различных типов и способов организации несанкционированных проникновений в чужие сети за последние годы значительно увеличилось, системы обнаружения атак (СОА) стали необходимым компонентом инфраструктуры безопасности большинства организаций. Этому способствуют и огромное количество литературы по данному вопросу, которую потенциальные злоумышленники внимательно изучают, и все более изощренные методы и сложные подходы к обнаружению попыток взлома информационных систем.

Для определения несанкционированных проникновений в сеть используется метод обнаружения аномалий. Данный метод заключается в определении ненормального (необычного) поведения на хосте или в сети. Можно предположить, что атаки отличаются от «нормальной» деятельности и могут, следовательно, быть определены системой обнаружения. Построение процедуры, которая бы позволила определять наличие либо отсутствие атаки, является актуальной задачей.

II. Подход к обнаружению вторжений путем определения характеристик невязки

Постановка данной задачи состоит в следующем: в дискретные моменты времени наблюдаются выборочные значения случайного процесса функционирования сети *y(k)*, *k = 1,2…N*. Рассматриваем возможность появления двух гипотез, H_0 и H_1, где H_0 соответствует состоянию, при котором все значения *y(k)* подходят модели нормальной работы сети, а H_1 предполагает, что на каком-то промежутке времени возникает аномалия. Требуется установить, какая из гипотез истинна.

Для этого необходимо провести рекурсивную оценку процесса функционирования сети. Суть рекурсивных процедур в том, что по полученному на k-м шаге значению $x(k)$ вычисляется последующее значение на $(k+1)$-м шаге. Далее значение на $(k+2)$-м шаге вычисляется по полученным на $(k+1)$-м шаге. То есть последующие значения вычисляются по предыдущим, но с учетом новых, очередных результатов наблюдения. Рекурсивная оценка – это процедура вычисления условного среднего $\hat{x}(t)/y(t)$, где $y(t)$ — наблюдение.

На выходе сети наблюдаем реализацию процесса *y(k)*

$$y(k) = H(k)x(k) + v(k) \qquad (1)$$

где *y(k)* — гауссовский марковский процесс, $H(k)$ — матрица усиления или ослабления сигнала $x(k)$, $v(k)$ — г.б. шум наблюдения.

Производим оценку данного процесса. Задача оценки состояния $\hat{x}(t)$, сопровождающая задачу управления и являющаяся ее составной, так же должна быть динамической во времени. Состояние динамических процедур моделируется дифференциальными или разностными уравнениями, что определяет их рекурсивный характер:

$$x(k+1) = F(k+1,k)x(k) + G(k+1,k)\xi(k),$$

2013 23rd Int. Crimean Conference "Microwave & Telecommunication Technology" (CriMiCo'2013). 9—13 September, Sevastopol, Crimea, Ukraine
 ISBN: 978-966-335-395-1. IEEE Catalog Number: CFP13788

где k — шаг дискретизации, который может выполняться во времени $k_t = t_n - t_{n-1}$, $\xi(k)$ — порождающий гауссовый белый шум.

В данной работе предлагается использовать оптимальную оценку такого процесса по наблюдению согласно формализованной процедуре оценки (фильтру Калмана-Бьюси). Данная процедура определяется соотношением:

$$\hat{x}(k+1) = F(k+1,k)\hat{x}(k) + \\ + K(k)\left[H(t)F(k+1,k)\hat{x}(k) - y(k)\right], \quad (2)$$

Известно [2], что в процедурах стохастической линейной оценки типа фильтра Калмана-Бьюси (2) используется невязка, разница между оценкой случайного процесса и его текущим значением:

$$\mu = H(t)F(k+1,k)\hat{x}(k) - y(k) \quad (3)$$

При гауссовой ситуации данная разница имеет название «обновляющего» процесса, который имеет свойства гауссовского белого шума (ГБШ). Таким образом анализируя невязку можно получить два возможных результата, приведенные ниже.

1. При наличии полезного сигнала (1) невязка соответствует параметрам ГБШ.

2. При наличии кроме полезного сигнала еще и постороннего невязка отлична от ГБШ.

III. Выбор критерия для определения принадлежности невязки к гауссову белому шуму

Определять, является ли сигнал на выходе невязки гауссовым белым шумом, возможно различными методами. Параметрическими — через отношение правдоподобия, и непараметрическими — с помощью порядковых статистик. Преимуществами непараметрических методов является их независимость от распределений, отсутствие необходимости наличия априорных данных и возможность организовывать корреляционный ряд из выборочных значений.

Этот корреляционный ряд при H_0 представляет собой неопределенную последовательность, а при H_1 коррелированную последовательность. Задачу сравнения последовательности выборки значений обновляющего процесса с гауссовым белым шумом решаем с помощью рангового критерия Уилкоксона.

Для реализации критерия мы находим разности, сдвиги между значениями признака на каждой из *n* пар измерений, выбрасываем из рассмотрения нулевые разности и находим ранги модулей разностей. Затем в качестве статистик Уилкоксона используем сумму рангов положительных и сумму рангов отрицательных разностей. Закон распределения этих статистик в предположении об отсутствии сдвига (нуль-гипотеза) известен, и можно найти критические значения наибольшей или наименьшей из сумм, а также эмпирические значимости.

Данный критерий позволяет сравнить 2 последовательности и обнаружить их принадлежность к одному случайному процессу либо к разным с заданным значением ранга.

Гауссов белый шум задаем как:

$$x(n) = k_1 e(n) + kx(n-1), \quad (4)$$

где $k_1 = \sqrt{D(1-k_2^2)}, k_2 = \exp(-a)$.

Итак, мы имеем ряд выборочных значений обновляющего процесса y_{Ii} и ряд случайных значений гауссового белого шума y_{IIi}. Вычислив разности $y_{Ii} - y_{IIi}$, $i = \overline{1,N}$ и упорядочив их по абсолютной величине, присваиваем каждой разности соответствующий ранг R_i; R_i — целое число и $R_i = \overline{1,N}$. Каждому рангу R_i приписывается знак соответствующей разности пары наблюдений $y_{Ii} - y_{IIi}$ и вычисляется сумма положительных рангов T_N. Значения вероятностей $P\{T_N \le a\}$ сводятся в таблицы где *a* — значение ранга T_N, взятое из таблиц в соответствии с количеством данных имитационных расчетов и выбираемым уровнем значимости α.

Проверка исходной гипотезы применительно к задаче дискриминации трактуется как проверка гипотезы об однородности выборок данных имитационных экспериментов y_{Ii} и y_{IIi}.Это соответствует принадлежности выборок одной генеральной совокупности, или данные, полученные из значений обновляющего процесса, статистически эквивалентны данным, полученным при моделировании гауссового белого шума. Гипотеза отвергается, если

$$P\{T_N \le a\} \ge 1 - \alpha.$$

IV. Заключение

В работе предложен метод обнаружения вторжений в телекоммуникационные системы путем анализа характеристик невязки, вычисляющейся при проведении рекурсивной оценки случайного процесса функционирования сети с помощью фильтра Калмана-Бьюси. Рассматривается гипотеза, что в отсутствии аномального воздействия невязка соответствует параметрам гауссового белого шума. В качестве критерия для определения корреляции невязки и гауссового белого шума в работе предлагается использовать ранговый критерий Уилкоксона. В случае, если гауссов белый шум и выборка значений обновляющего процесса коррелируются — то принимается решение об отсутствии вторжений в систему. В случае же приобретения выборкой определенной закономерности фиксируется аномальное воздействие.

IV. References

[1] Mironov M.A. Obnaruzhenie izmenenij svojstv nabljudaemyh i nenabljudaemyh processov [Detection of properties changing of observed and unobservable processes]. *Radiotehnika*, 2007, No 1.

[2] Popovskij V.V., Olejnik V.F. Matematicheskie osnovy upravlenija i adaptacii v telekommunikacionnyh sistemah [Mathematical basis control and adaptation at telecommunication systems]. H. SMIT, 2011. 362 p.

[3] Gaek Ja., Shidak Z. Teorija rangovyh kriteriev [Theory of range criteria]. Moscow, Nauka, 1971. 376 p.