Максимовский А.Ю.

О параметрах управления в одной модели мониторинга информационной безопасности сложных систем

Аннотация: В докладе рассмотрены свойства модели мониторинга состояния информационной безопасности сложных систем с использованием аппарата цепей Маркова. Предложены новые подходы к выбору параметров контроля защищенности сетевых объектов, входящих в состав сложных систем.

Ключевые слова: мониторинг информационной безопасности, цепи Маркова

Мониторинг устойчивого (безопасного) функционирования входящих в сложные системы сетевых объектов, как правило, представляет собой комплекс процедур анализа временны́х рядов событий, происходящих с объектом контроля. При этом, на состояние объекта контроля влияют внешние факторы (воздействия, атаки), так и действия, предпринимаемые в целях нейтрализации негативным внешним воздействиям, определяемые в зависимости от текущего состояния (уровня защищенности) объекта контроля. Таким образом, возникают два временных информационных потока: воздействий на объект мониторинга $x_1, x_2, \dots, x_t, \dots$ и оценок его состояний: $s_1, s_2, \dots, s_t$. Вообще говоря, оценка s_t вычисляется с учетом значений $s_{t-k}, s_{t-k+1}, \dots, s_{t-1}$ и x_t, где k – параметр, характеризующий глубину (зависимость во времени) учета предыдущих событий. При этом в качестве x_t может использоваться некоторый параметр, при формировании которого целесообразно учитывать как собственно внешние воздействия в рассматриваемый момент функционирования на объект контроля, так и действия, предпринимаемые для его защиты от негативных воздействий. В итоге мы получаем функциональную зависимость

$$s_t = M(s_{t-k}, s_{t-k+1}, \dots, s_{t-1}, x_t), \quad (1)$$

которую можно рассматривать как базовую при решении задачи оценки защищенности объекта контроля и эффективности его мониторинга.

Формула (1) является одним из вариантов задания авторегрессии и имеет много общего с функцией переходов неавтономного регистра сдвига длины k. Поэтому использование автоматных моделей регистрового типа является актуальным для формирования общего подхода для мониторинга информационной безопасности (далее – ИБ) как произвольных сетевых объектов, так и объектов, автоматными моделями которых являются собственно регистрами сдвига. Автоматно-алгебраические свойства этих моделей подробно рассматривались в работах [1-2]. Поэтому представляет интерес исследовать перспективы использования результатов, полученных в [3] при изучении схемы авторегрессии на конечной абелевой группе, управляемой марковской последовательностью, и ее аналогов, включая такие, для которых удается найти удобные для практического использования виды формулы (1), форматы параметров $x_1, x_2, \dots, x_t, \dots$ и $s_1, s_2, \dots, s_t$, а также виды их взаимной зависимости.

Рассмотрим ситуацию, когда функция M определяется соотношением

$$s_{t+1} = \left[\frac{s_t + x_t}{d}\right], \tag{2}$$

где $d|m$, $[u]$ – целая часть числа u, $\{s_t\} \in \Omega_m = \{0, \dots, m-1\}$, $t \geq 0$, $\{x_t\}$ – последовательность независимых одинаково распределенных на множестве Ω_m случайных величин, которые имеют равномерное распределение этом множестве. Очевидно, определенная таким образом последовательность $\{s_t\}$ является цепью Маркова [4]. Заметим, что рассматриваемая модель мониторинга защищенности предполагает проведение предварительной классификации внешних воздействий и соответствующих оценок защищенности объекта контроля (такого рода классификация была предложена и использована в [5] для оценки эффективности одной модели контроля защищенности сложных систем.

Для удобства перепишем соотношение (2) в эквивалентном виде

$$s_{t+1} = \left[\frac{s_t + x_t}{d}\right] + X_t(y_t) \pmod{m}, \tag{3}$$

где $X_t = (X_t(0), \dots, X_t(m-1))$ – последовательность независимых случайных векторов, компоненты которых $X_t(nd + +k), n = 0{,}1 \dots, \frac{m}{d} - 1, k = 0{,}1, \dots, d-1,$ имеют распределение

$$\mathcal{P}(X_t(nd+k) = \begin{cases} \frac{d-k}{m}, l = 0, \\ \frac{d}{m}, l = 1, \dots, \frac{m}{d} - 1, \frac{k}{m}, l = \frac{m}{d}, \\ 0, l > \frac{m}{d} \end{cases}$$

Ниже мы получим рекуррентные соотношения для предельных вероятностей состояний цепи (3), рекуррентную формулу, позволяющую вычислить характеристический многочлен матрицы A_m переходных вероятностей цепи (3), имеющей m состояний $\{0, \dots, m-1\}$, и максимальное отличное от единицы собственное число этой матрицы.

Структура матрицы A_m и результат теоремы 13.III из [4] позволяют сделать вывод о том, что цепь (3) обладает стационарным распределением $\vec{q} = (q(0), \dots, q(m-1))$. При этом цепь (3) имеет один эргодический класс, и можно провести классификацию ее состояний цепи путем нахождения ненулевых вероятностей в стационарном распределении. Основные свойства этого распределения содержит следующее утверждение.

Утверждение 1. 1. Справедлива формула

$$q(s) + q\left(\frac{m}{d} + s\right) = \frac{d}{m}, 0 \le s \le \frac{m}{d} - 1 \quad (4)$$

2. При условии $d^{r+1} | m, r \ge 1,$ для любого $k, 0 \le k \le d-1$ справедливо равенство

$$\sum_{s=0}^{d^{r-1}-1} \sum_{l=0}^{m'-1} q(ld^r + kd^{r-1} + s) = \frac{1}{d}, \quad (5)$$

где $m' = \frac{m}{d^r}$.

Замечание 1. Если $d^2 \nmid m$, то (5) не выполняется. Например, при $m = 6$ и $d = 2,$ $\vec{q} = \left(\frac{1}{15}, \frac{4}{15}, \frac{1}{3}, \frac{4}{15}, \frac{1}{15}, 0\right)$, но при этом $\sum_{l=0}^{2} q(2l) = \frac{7}{15}, \sum_{l=0}^{2} q(2l+1) = \frac{8}{15}$.

Перейдем к классификации состояний цепи (3).

Утверждение 2. Состояния цепи (3) с номерами, большими $\left[\frac{m-1}{d-1}\right] - 1$, являются несущественными. Все остальные состояния этой цепи существенные.

Здесь $[x]$ – наименьшее целое, не меньшее x.

Следствие 1. 1. Если $\left\lceil\frac{m-1}{d-1}\right\rceil - \frac{m}{d} \le s \le \frac{m}{d} - 1$, то $q(s) = \frac{d}{m}$.

2. При $d \to \infty, \frac{m}{d} \to \infty$, почти все существенные состояния цепи (3) имеют одинаковые предельные вероятности, равные $\frac{d}{m}$.

Пусть ξ – случайная величина с распределением $\mathcal{P}(\xi = s) = q(s), s \in \Omega_m$. Вычислим математическое ожидание и дисперсию этой случайной величины.

Утверждение 3. Имеет место равенства:

1) $\mathrm{M}\xi = \frac{m-d}{2(d-1)}$,

2) $\mathrm{D}\,\xi = \frac{m^2+d^2-2}{12(d-1)}$, если $d^2|m$.

Замечание 1. Если $d^2 \nmid m$, то равенства п. 2 утверждения 3 не имеет места. Пример: $m = 6, d = 2, \vec{q} = \left(\frac{3}{8}, \frac{1}{2}, \frac{1}{8}, 0,0,0\right)$. Тогда $\mathrm{D}\xi = \frac{7}{16}$, но $\frac{m^2+d^2-2}{12(d-1)} = \frac{43}{48}$.

Приведем результаты о свойствах характеристического многочлена $\chi_m(\lambda)$ матрицы A_m.

Утверждение 4. 1. Если $d^2|m$, то справедлива рекуррентная формула

$\chi_m(\lambda) = d^{-m'}(\lambda - 1)\lambda^{m-m'-1}\chi_{m'}(d\lambda)$.

2. Если $d \ge m'$, то $\chi_m(\lambda) = (\lambda - 1)\left(\lambda - \frac{1}{d}\right)\lambda^{m-2}$.

Следствие 2. 1. Если $m = d^r$, то $\chi_m(\lambda) = (\lambda - 1)\left(\lambda - \frac{1}{d}\right) \dots (\lambda - \frac{1}{d^r})\lambda^{m-r-1}$.

2. Если $d^2|m$ или $d^2 \ge m$, то максимальное отличное от 1 собственное значение матрицы A_m равно $\frac{1}{d}$.

Заключение

Приведенные выше результаты позволяют сделать следующие выводы:

1) эффективная классификация входных воздействий при выборе гармоничных оценок защищенности позволяет получить сведения, необходимые для прогнозирования поведения объекта контроля, как это удалось сделать выше;

2) при выборе модели, определяющей влияние на состояния объектов системы входных воздействий, могут использоваться и

регрессионные [6], и авторегрессионные модели (в зависимости от свойств алгебры, над которой строятся такие модели, и природы внешних воздействий);

3) переход к векторному представлению модели управления (переход от соотношения (2) к его эквивалентному виду (3)) оказался весьма плодотворным и позволил получить все базовые результаты о свойствах соответствующей цепи Маркова; поэтому целесообразно и в дальнейшем применять векторных модели при разработке параметров мониторинга ИБ.

Литература:

1. *Калашников А.О., Максимовский А.Ю.* Использование специальных соотношений в автоматах для мониторинга информационной безопасности сетевых объектов//Информация и безопасность. – 2019. – Т. 22. № 1 (1). – С. 30-37.

2. *Калашников А.О., Максимовский А.Ю.* Развитие автоматных моделей мониторинга информационной безопасности сетевых объектов//Информация и безопасность. – 2019. – Том 22. № 4 (4). – С. 549-556.

3. *Круглов И.А*. Авторегрессия на конечной абелевой группе с марковской входной последовательностью//Математические вопросы криптографии. – 2011. – Т. 2. №4. – С. 25-36.

4. *Романовский В.И.* Дискретные цепи Маркова. – М.–Л.: Гостехиздат, 1949. – 436 с.

5. *Калашников А.О., Максимовский А.Ю.* Об оценке эффективности аддитивной ролевой модели контроля защищенности систем//Информация и безопасность. – 2019. – Т. 22. № 1 (4). – С. 22-29

6. *Дрейпер Н., Смит Г.* Прикладной регрессионный анализ. Книга 1. – М.: Финансы и статистика, 1986. – 366 с.

Нестеров В.С., Безгубова Ю.К.

Особенности применения ситуационно-контекстной визуализации в системах мониторинга и управления

Аннотация: Рассматриваются вопросы использования в системах мониторинга и управления ситуационно-контекстной визуализации, являющейся конкретным