УДК 004.7 (043.2)

Нагурный А.А.

ОЦЕНИВАНИЕ ПАРАМЕТРОВ И СОСТОЯНИЯ АВТОНОМНОГО СЕГМЕНТА КОРПОРАТИВНОЙ СЕТИ

Институт компьютерных технологий
Национального авиационного университета

Рассмотрен метод идентификации автономного сегмента сети с запаздыванием и ошибками передачи служебной информации. Показано, что внутренние и внешние возмущения и помехи по-разному влияют на состояние сетевого сегмента. Предложено использовать модель регенеративного процесса возникновения аномалий, вызванных отказами и внешними возмущениями. Для решения обратной задачи идентификации применен байесовский подход. На основе представления сети как системы с квазистационарным состоянием на интервале наблюдения разработан алгоритм распознавания локальных классов аномалий

Введение

Система управления компьютерной сетью масштаба корпорации технически представляет собой набор средств обмена информацией и взаимодействия распределенных приложений в гетерогенной среде. По существу, она является сложной системой, к которой применимы методы системного анализа.

При управлении сетями необходимо решать следующие задачи:

– обмена информацией о целях управления в сети;

– передачи и обработки информации о результатах управления;

– выработки решений на основе результатов анализа информации о результатах управления;

– передачи информации о результатах принятых решений и собственно управления.

Таким образом, для управления необходимо иметь информацию о параметрах и состоянии объекта, условиях его функционирования, действующих на объект возмущений, анализировать изменения состояния управляемого объекта под влиянием управляющих действий.

Существующие системы управления сетями, несмотря на их функциональную избыточность, не имеют в своем составе средств оценки и прогноза поведения компьютерной сети. Большинство средств управления в действительности сетью не управляет, а всего лишь пассивно осуществляет ее мониторинг, фиксируя постфактум только аномальные состояния. Необходимо в реальном масштабе времени решать задачи анализа, прогноза и предотвращения возможных сбоев и аномалий в работе сетевых узлов и компьютерной сети в целом. Такая система управления нужна, особенно для работы в условиях критичного применения – при больших перепадах вычислительной нагрузки на терминальные узлы и информационной нагрузки на каналы передачи.

Оценивание параметров и состояний сегмента сети

Оценивание статистических характеристик внешних возмущений, действующих на систему, и внутренних помех (идентификация возмущений и помех) является необходимым условием текущей коррекции динамических характеристик системы и обеспечения ее помехоустойчивости, а, в конечном счете – гарантии требуемых показателей функционирования системы.

Указанный анализ статистических характеристик применительно к сети позволяет определить такие принципиально важные для управления ситуации, как перегрузки в отдельных звеньях сети, выход их из строя, задержки в передаче общей информации, сигналов управления и т. д.

В качестве математической модели системы управления автономным сегмен-

том сети используем одномерную линейную систему. Рассмотрим задачу идентификации не коррелированных с входным сигналом помех в такой системе. При этом предполагается статистическая независимость процессов, протекающих в разных сегментах сети. Модель системы управления представлена на рис. 1.

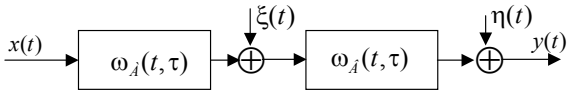

Рис. 1. Модель системы управления

Полагаются известными:

– импульсная характеристика системы в целом $\omega(t,\tau)$ и ее отдельных звеньев $\omega_F(t,\tau)$ и $\omega_B(t,\tau)$;

– измеренные значения сигналов $x(t)$ и $y(t)$ и их средние значения (математические ожидания) $m_x(t)$, $m_y(t)$ и корреляционные функции $K_x(t_1,t_2)$ и $K_y(t_1,t_2)$.

В соответствии с рассматриваемой задачей необходимо определить статистические характеристики помех $\xi(t)$ или $\eta(t)$, где

$$\eta(t) = \int_0^t \omega_B(t,\tau) n(\tau) d\tau .$$

Для приведенной к выходу помехи $\eta(t)$:

$$y(t) = \int_0^t \omega(t,\tau) x(\tau) d\tau + \eta(t) .$$

С учетом некоррелированности входного сигнала (управляющей информации) и помехи связь между корреляционными функциями входного сигнала, выходного сигнала и помехи имеет вид [3]

$$K_y(t_1,t_2) = \int_0^{t_1}\int_0^{t_2} \omega(t_1,\tau)\omega(t_2,\nu) k_x(\tau,\nu) d\tau d\nu + K_N(t_1,t_2) .$$

Отсюда искомое выражение для корреляционной функции приведенной помехи $N(t)$

$$K_N(t_1,t_2) = K_y(t_1,t_2) - \int_0^{t_1}\int_0^{t_2} \omega(t_1,\tau)\omega(t_2,\nu) k_x(\tau,\nu) d\tau d\nu .$$

Для случая стационарной системы имеем: $m_N = m_y - \int_0^\infty \omega(\tau) m_x(\tau) d\tau$;

$$K_N(\mu) = K_y(\mu) - \int_0^\infty\int_0^\infty \omega(\tau)\omega(\nu) k_x(\mu+\tau-\nu) d\tau d\nu ;$$

$$S_N(\omega) = S_y(\omega) - \left|w(j\omega)\right|^2 S_x(\omega) ,$$

где $S(\omega)$ и $w(j\omega)$ – спектральная плотность и частотная характеристика соответственно.

Для структурно локализованной помехи $n(t)$ и стационарной системы соответствующие характеристики m_n, $K_n(\tau)$ и $S_n(\omega)$ имеют вид [3].

$$m_n = \frac{m_y}{w_B(jD)} - w_A(jD) m_x , \quad (1)$$

$$K_n(\mu) = \int_0^\infty\int_0^\infty \overline{\omega}_B(\tau)\overline{\omega}_B(\nu) k_y(\mu+\tau-\nu) d\tau d\nu - \int_0^\infty\int_0^\infty \omega_A(\tau)\omega(\nu) k_x(\mu+\tau-\nu) d\tau d\nu , \quad (2)$$

где $\overline{\omega}_B(\tau)$ – импульсная характеристика, обратная $\omega_B(\tau)$.

$$S_n(\omega) = \frac{S_y(\omega)}{\left|w_B(j\omega)\right|^2} - \left|w_A(j\omega)\right|^2 S_x(\omega). \qquad (3)$$

В качестве примера рассмотрим определение m_n и $k_n(\tau)$ в стационарной системе (рис. 1), имеющей:

– передаточные функции звеньев

$$w_A(j\omega) = \frac{K_A(T_A j\omega + 1)}{T_1 j\omega + 1},$$

$$w_B(j\omega) = \frac{K_B}{T_B j\omega + 1};$$

– статистические характеристики входных $x(t)$ и выходных сигналов m_x=const; m_y=const;

$$K_x(\tau) = D_x e^{-\alpha_x|\tau|};\ K_y(\tau) = D_y e^{-\alpha_y^2\tau^2}.$$

Статистические характеристики помехи определяются в соответствии с (1 – 3): $m_n = \frac{m_y}{K_B} - K_A m_x$.

Для определения $S_n(\omega)$ по известным корреляционным функциям входного и выходного сигналов найдем их спектральные плотности

$$S_x(\omega) = D_x \frac{2\alpha_x}{\alpha_x^2 + \omega^2},$$

$$S_y(\omega) = D_y \sqrt{\frac{\pi}{\alpha_y^2}} e^{-\omega^2/4\alpha_y^2}$$

и квадраты модулей передаточных функций звеньев

$$\left|w_A(j\omega)\right|^2 = K_A^2 \frac{T_A^2\omega^2 + 1}{T_1^2\omega^2 + 1},$$

$$\left|\frac{1}{w_B(j\omega)}\right|^2 = \frac{T_B^2\omega^2 + 1}{K_B^2}.$$

Спектральная плотность помехи $n(t)$ в соответствии с выражением (3) определяется как

$$S_n(\omega) = \frac{D_y}{K_B^2}\frac{\sqrt{\pi}}{\alpha_y^2} e^{-\omega^2/4\alpha_y^2}(1 + T_B\omega^2) - D_x K_A^2 \frac{2\alpha_x(T_A^2\omega^2 + 1)}{(\alpha_x^2 + \omega^2)(T_1^2\omega^2 + 1)}. \qquad (4)$$

При определении импульсных характеристик обратных систем в соответствии с (2) для нахождения $K_n(t)$ необходимо тщательно анализировать вид корреляционной функции для того, чтобы избежать сингулярностей. Считая, что в помехе всегда присутствует компонент белого шума (следовательно, сингулярности отсутствуют), можно применить теорему Винера-Хинчина:

$$K_n(t) = \frac{1}{2\pi}\int_{-\infty}^{+\infty} S_n(\omega) e^{j\omega\tau} d\omega.$$

Для спектральной плотности (4) корреляционная функция помехи имеет вид (для T_0=1)

$$K_n(\tau) = D_y[1 + 2\alpha_y^2(1 - 2\alpha_y^2\tau^2)]e^{-\alpha_y^2\tau^2} - C(A_1 e^{-\alpha_x|\tau|} + a_2 e^{-\frac{1}{T_1}|\tau|}),$$

где $C = \frac{2K_A^2 D_x \alpha_x T_A^2}{T_1^2}$;

$$A_1 = \left[\frac{(\alpha_x - \frac{1}{T_A})^2}{2\alpha_x(\alpha_x - \frac{1}{T_1})^2} + \frac{(\alpha_x - \frac{1}{T_A})(\frac{1}{T_A} - \frac{1}{T_1})}{(\alpha_x - \frac{1}{T_1})^2(\alpha_x + \frac{1}{T_1})}\right];\ A_2 = \left[\frac{(\frac{1}{T_A} - \frac{1}{T_1})^2}{2\frac{1}{T_1}(\alpha_x - \frac{1}{T_1})^2} + \frac{(\alpha_x - \frac{1}{T_A})(\frac{1}{T_A} - \frac{1}{T_1})}{(\alpha_x - \frac{1}{T_1})^2(\alpha_x + \frac{1}{T_1})}\right]$$

Определение состояния сети по зафиксированному возмущению производится методами статистического распознавания.

При байесовском подходе к решению задачи распознавания, как известно, достигается минимум среднего риска. В соответствии с байесовским критерием вычисляются условные апостериорные вероятности отнесения объекта к тому или иному классу. Решение принимается на основании сравнения значений вычисленных апостериорных вероятностей. Однако для применения байесовского подхода необходимо иметь полную априорную информацию о статистических характеристиках мешающих воздействий, что может иметь место лишь в исключительных случаях. В условиях неполноты априорной информации наиболее целесообразно применять метод максимума правдоподобия, дающий эффективные оценки в широком классе априорных распределений.

Если объект характеризуется N признаками x_j, $j=1,\ldots,N$, и признаки распознаваемого объекта принимают значения $x_1 = x_1^0, x_2 = x_2^0, \ldots, x_N = x_N^0$, задача сводится к проверке сложной гипотезы против сложной альтернативы. Вероятность того, что при осуществлении события $a_N=(x_1^0, x_2^0, \ldots, x_N^0)$ объект относится к Ω_i классу из m, равна

$$P(\Omega_i / a_N) = \frac{P(\Omega_i) f_i(x_1^0, x_2^0, ..., x_N^0)}{\sum_{i=1}^{m} P(\Omega_i) f_i(x_1^0, x_2^0, ..., x_N^0)},$$

где $P(\Omega_i / a_N)$ – апостериорная вероятность отнесения объекта к классу Ω_i при осуществлении события a_N; $P(\Omega_i)$ – априорная вероятность появления объекта класса Ω_i; $f_i(x_j)$ – многомерные условные плотности распределения вероятностей значений признаков по классам.

Решающее правило для случая двух классов Ω_1 и Ω_2 отнесения объекта к классу Ω_1 запишется в виде

$$\frac{P(\Omega_1 / a_N)}{P(\Omega_2 / a_N)} > \frac{C_2}{C_1}$$

или

$$\frac{f_2(a_N)}{f_1(a_N)} > \frac{C_1 P(\Omega_1)}{C_2 P(\Omega_2)}, \qquad (5)$$

где C_1 и C_2 – ошибки первого и второго рода; $\frac{C_1 P(\Omega_1)}{C_2 P(\Omega_2)} = \lambda_0$ – пороговое значение коэффициента правдоподобия.

В соответствии с методом максимального правдоподобия зададим пороговое значение ошибки первого рода (уровень значимости критерия) и будем стремиться минимизировать ошибку второго рода, т.е. максимизировать мощность критерия. В такой постановке решающее правило (критерий) сводится к известному критерию Неймана-Пирсона.

Рассмотрим методику применения алгоритма распознавания на следующем частном примере. Пусть нормированная корреляционная функция возмущения, действующего на объект, аппроксимируется выражением $\rho(\tau) = e^{-\alpha|\tau|}\cos\beta\tau$. В качестве признака для оценки одного из двух состояний объекта Ω_1 и Ω_2 возьмем параметр α, считая его распределенным по закону Гаусса с параметрами $m_{\alpha i}$ и $\sigma_{\alpha i}$, $i=\overline{1,2}$. Состояние Ω_1 характеризуется параметрами $m_{\alpha 1}$ и $\sigma_{\alpha 1}$, а состояние Ω_2 – параметрами $m_{\alpha 2}$ и $\sigma_{\alpha 2}$ соответственно.

Граничное значение параметра α найдем из условия:

$$\frac{f_2(\alpha)}{f_1(\alpha)} = \frac{C_1 P(\Omega_1)}{C_2 P(\Omega_2)} = \lambda_0.$$

$$\frac{\exp\left[-(\alpha - m_{\alpha 2})^2 / 2\sigma_{\alpha 2}^2\right]}{\exp\left[-(\alpha - m_{\alpha 1})^2 / 2\sigma_{\alpha 1}^2\right]} = \lambda_0 \frac{\sigma_{\alpha 2}}{\sigma_{\alpha 1}};$$

$$\alpha^2 A + \alpha B + C = 0, \qquad (6)$$

где

$$A = \left(\frac{1}{2\sigma_{\alpha 1}^2} - \frac{1}{2\sigma_{\alpha 2}^2}\right);\ B = \left(\frac{m_{\alpha 2}}{\sigma_{\alpha 2}^2} - \frac{m_{\alpha 1}}{\sigma_{\alpha 1}^2}\right);$$

$$C = \frac{m_{\alpha 1}^2}{2\sigma_{\alpha 1}^2} - \frac{m_{\alpha 2}^2}{2\sigma_{\alpha 2}^2} - \ln\lambda_0 \frac{\sigma_{\alpha 2}}{\sigma_{\alpha 1}}.$$

Решая квадратное уравнение (6), находим предельное значение α. Путем сравнения измеренного значения α^0 с предельным, т. е. определения знака неравенства выражения (5), определяем класс распознаваемого объекта.

Выводы

Таким образом, алгоритм распознавания класса возмущений для прогнозирования состояния сети сводится к выполнению таких операций:

– оценивание постоянной времени корреляционной функции возмущения;

– последовательное оценивание максимума отношения правдоподобия (5).

Другими словами, решается задача комбинирования по максимуму отношения правдоподобия. Практическая реализация устройств комбинирования по максимуму отношения правдоподобия аппаратными или программными методами не представляет труда [6]. Обычно для задач комбинирования для выбора максимума из набора данных используют иерархические бинарные схемы.

Список литературы

1. *Сейдж Э., Мелс Дж.* Теория оценивания и ее применение в связи и управлении.: Пер. с англ. Под ред. проф. Б.Р. Левина. – М.: Связь, 1976. – 496 с.

2. *Эйкхофф П.* Основы идентификации систем управления // Пер. с англ. под ред. Н.С. Райбмана. – М.: Мир, 1975. – 684 с.

3. *Гельфандбейн Я.А., Колосов Л.В.* Ретроспективная идентификация возмущений и помех. – М.: Советское радио, 1972. – 232 с.

4. *Свешников А.А.* Прикладные методы теории случайных функций. – М.: Наука, 1968. – 463 с.

5. *Горелик А.Л., Скрипкин В.А.* Методы распознавания. Учебное пособие для вузов. – М.: Высшая школа, 1977. – 222 с.

6. *Ван Трис Г.* Теория обнаружения, оценок и модуляции. Том 1. Теория обнаружения, оценок и линейной модуляции. – Пер. с англ., под ред. проф. В.И. Тихонова. – М.: Советское радио, 1972. – 744 с.

7. *F. Cohen*. Computer Viruses: theory and experiments // DOD/NBS 7th Conference on Computer Security (1984); Computers and Security, 1987. – Vol. 6#1. – P. 22–35.

8. *Леман Э.* Проверка статистических гипотез. – М.: Наука, 1979. – 408 с.

9. *Левин Б.Р.* Теоретические основы статистической радиотехники, книга вторая. – М.: Сов. радио, 1968. – 504 с.

10. *Вальд А.* Последовательный анализ. – М.: Физматгиз, 1960. – 606 с.

Подано до редакції 30.04.10