УДК 004.738 (043.3)

Данилина Г.В., к.т.н.,
Милокум Я.В., к.т.н.,
Безвершенко Э.И.

ИДЕНТИФИКАЦИЯ ПАРАМЕТРОВ СЕТЕВОЙ АТАКИ ДЛЯ РАЦИОНАЛЬНОГО РАСПРЕДЕЛЕНИЯ РЕСУРСОВ ЗАЩИТЫ

Национальный авиационный университет

Для непрерывного оценивания параметров и состояния сети в реальном времени сеть рассматривается как дискретная динамическая система с сосредоточенными параметрами. Пошаговая идентификация параметров и состояния сети на основе дискретного фильтра Калмана сводится к решению задачи оценивания корреляционной матрицы и переходной матрицы состояния системы

Постановка задачи

В настоящее время активно разрабатываются и внедряются системы нового поколения для сбора информации и локализации экстремальных ситуаций сетей [1, 2]. Современная система сбора информации о функционировании корпоративной сети, помимо обнаружения и распознавания экстремальных (нештатных) ситуаций, возникающих, например, из-за действий злоумышленников, должна осуществлять полный мониторинг сети в целом и отдельных ее сегментов. Другими словами, необходимо в реальном времени решать задачу непрерывного оценивания параметров и состояния сети, т.е. задачу идентификации.

Отдельный сегмент сети рассматривается как динамическая система смешанного типа, которая характеризуется неким функционалом качества *ΨQ*, зависящим от множества параметров сети. К ним, в частности, относятся параметры сетевых (СУ) и терминальных (ТУ) узлов – лояльных партнеров, совместно с которыми создается распределенная система защиты.

Параметры линий передачи данных в рамках рассматриваемой задачи наиболее целесообразно оценивать опосредованно, по результатам анализа входных сигналов соседних узлов. При этом, очевидно, необходимо отдельно анализировать параметры при прохождении трафика как от (*i*-1)-го к *i*-му узлу, так и обратно, поскольку в направлениях «туда» и «обратно» параметры линии передачи не обязательно идентичны. Однако можно рассматривать анализируемые параметры как дополнительные сосредоточенные параметры сети.

Таким образом, необходимо разработать метод и построить алгоритм идентификации участка сети как дискретной динамической системы с сосредоточенными параметрами.

Параметры и состояние сети в *k*-й момент времени описываются вектором состояния $X_{sk} = X_s(k/k-1)$ и матрицей состояния $\Phi_s(k,k-1)$. Без потери общности можно предположить, что число анализируемых и управляемых параметров в каждом из *N* узлов одинаково и равно МСУ. Число контролируемых параметров в *ТУj*-1 и *ТУj* обозначим МТУ. Тогда размерность вектора состояния *Xsk* равна $M_{\text{СУ}} \times N + 2M_{\text{ТУ}}$. Соответственно размерность матрицы состояния $\Phi_s(k,k-1)$ равна $\left[M_{\text{СУ}} \times N + 2M_{\text{ТУ}} \right] \times \left[M_{\text{СУ}} \times N + 2M_{\text{ТУ}} \right]$.

Поскольку изменения параметров и состояния отдельного узла практически не влияют на соответствующие характеристики других узлов, матрица $\Phi_s(k,k-1)$ является приближенно блочно-диагональной. Она содержит *N* + 2 блока: два блока размерностью $M_{\text{ТУ}} \times M_{\text{ТУ}}$ (верхний и нижний блоки) и *N* промежуточных блоков размерностью $M_{\text{СУ}} \times M_{\text{СУ}}$.

Следовательно, общая задача идентификации участка сети распадается на совокупность частных задач идентификации отдельных узлов.

Представим математическую модель узла в виде стохастического линейного разностного уравнения n-го порядка, решением которого в *k-й* момент времени является вектор текущего состояния *Xk*. Этим вектором полностью определяется состояние участка сети как динамической системы в данный момент времени. Пусть вектор состояния описывается уравнением

$$X_k = \phi(k,k-1)X_{k-1} + \lambda_k U_k + \xi_k, \qquad (1)$$

где $\phi(k,k-1)$ – матрица состояния размерности $n \times n$; λ_k – матрица управления размерности и $n \times j$, причем в рассматриваемом случае $j \le n$; U_k - детерминированный вектор управления размерности *n*; ξ_k - вектор случайных возмущений самой разной природы. Он также имеет размерность *n* и является случайным на каждом шаге *k*. Его компонентами, помимо атакующих воздействий, могут быть человеческий фактор (результаты действий злоумышленника, некомпетентность или утрата лояльности персонала), внешние и внутренние помехи и шумы, уходы параметров оборудования, полные и/или частичные отказы оборудования, ошибки передачи данных и др.

В общем случае распределение вероятности вектора ξ_k может быть произвольным, в том числе и полимодальным. Однако, учитывая эффект нормализации в сложных системах [3, 4], можно ограничиться гауссовым приближением для первых апостериорных плотностей вероятностей параметров рассматриваемого вектора. Кроме того, в результате решения уравнения (1) получают интегральную оценку и оценку апостериорного математического ожидания.

Учитывая приведенные выше соображения, примем распределение вектора ξ_k гауссовым с нулевым математическим ожиданием и неотрицательно определенной ковариационной матрицей *Qk* конечной нормы: $\xi_k \sim N[0, Q_k]$. Математическое ожидание ковариационной матрицы *Qk* есть $E[\xi_i \xi_k^T] = Q_k \delta_{ik}$, норма $\|Q_k\| < \infty, \ \forall k$, δ_{ik} - символ Кронекера, *E* – символ математического ожидания.

Матрица $\phi(k,k-1)$ обладает всеми свойствами переходной матрицы: $\phi^{-1}(k,k-1) = \phi(k-1,k) \quad \forall k$;

$$\phi(k,k-j) = \phi(k,l)\phi(l,k-j)$$

$$k \ge l \ge k-j; \quad \phi(k,k) = I$$

где *I* – единичная матрица.

Зададим начальное состояние вектора *X0, k = 0*. Считаем *X0* случайным вектором, распределенным по Гауссовскому закону с математическим ожиданием *q0* и неотрицательно определенной ковариационной матрицей *P0*, т.е. $X_0 \sim N[q_0, P_0]$.

Предполагаем, что результат наблюдения (измерения) представляет собой аддитивную смесь в виде суммы компонентов вектора состояния и шума:

$$y_k = M_k X_k + \eta_k, \qquad (2)$$

где y_k - вектор измерений размерности m, полученный в *к*-й момент времени, M_k - матрица с размерностью $m \times n$, а η_k - m-мерный вектор шумов измерения с нулевым математическим ожиданием и неотрицательно определенной ковариационной матрицей R_k: $\eta_k \sim N[0, R_k]$; $E[\eta_i \eta_k^T] = R_k \delta_{ik}$, $\|R_k\| < \infty, \quad \forall k$.

При заданных матрицах $\phi_k, Q_k, \lambda_k, R_k, M_k$ и начальных условиях q_0 и P_0 оптимальным решением задачи оценивания является фильтр Калмана [5] . Оптимальность здесь понимается в смысле получения сходящейся последовательности несмещенных и эффективных (с минимальной дисперсией) оценок

$\hat{X}_k$ состояния вектора X_k. Оценки получаются в виде линейных комбинаций измерений вектора y_j, $j=\overline{1,k}$.

Алгоритм фильтрации описывается следующей системой уравнений:

$$\begin{aligned}
&\hat{X}(k/k-1)=\phi(k,k-1)\hat{X}(k-1/k-1)+\lambda_k U_k\ ;\\
&P(k/k-1)=\phi(k,k-1)P(k-1/k-1)\phi^T(k,k-1)+Q_k\ ;\\
&K_k=P(k/k-1)M_k^T\left[M_kP(k/k-1)M_k^T+R_k\right]^{-1}\ v_k=y_k-M_k\hat{X}(k/k-1)\ ;\\
&\hat{X}(k/k)=\hat{X}(k-1/k-1)+K_kv_k\ ;\\
&P(k/k)=[I-K_kM_k]P(k/k-1)[I-K_kM_k]^T+K_kR_kK_k^T
\end{aligned} \qquad (3)$$

где через $\hat{X}(i/j)$ и $P(i/j)$ обозначены соответственно текущая оценка и ковариационная матрица ошибок оценивания в произвольный момент i при имеющихся наблюдениях в предыдущие моменты времени $\overline{1,j}$. Решение отыскивается при начальных условиях

$$\hat{X}(0/0)=q_0,\ P(0/0)=P_0. \qquad (4)$$

Вектор v_k, по существу, является невязкой измерений на *к*-м шаге, которая теоретически стремится к нулю при $k\to\infty$

Алгоритм оценивания (3) является оптимальным только при точном знании параметров векторов и матриц, входящих в уравнения (1 – 3), и начальных условий (4) [6]. Однако в нашем случае, как и в большинстве практических случаев [7], знание численных значений всех или нескольких элементов векторов и матриц является неполным.

При незначительном усложнении алгоритма можно организовать своего рода «активный режим» сбора данных: при возникновении нештатной ситуации на любом из сетевых узлов сигналам с этого узда дается высший приоритет, и система идентификации переходит на первоочередное обслуживание этого узла. В этом случае риск пропуска или неприемлемой задержки обнаружения нештатной ситуации сводится к минимуму.

Учитывая приведенные выше соображения, сформулируем задачу идентификации. Необходимо оценить состояние вектора X_k в уравнении (1) на основе последовательности, состоящей из k результатов измерений вектора y_i, $i=\overline{1,k}$. Оценки будут несмещенными и эффективными (в смысле минимума дисперсии) при точном знании матриц $\Phi\ k,k-1$, λ_k, Q_k, R_k, M_k, $\forall k$. Поскольку данное условие может быть выполнено лишь теоретически при $k\to\infty$, рассмотрим модели ошибок определения матриц.

Предположим, что точные значения матриц определяются следующими уравнениями (аргументы для краткости опущены):

$$\begin{aligned}
&\tilde{\phi}_k=\phi_k-\Delta\phi_k;\\
&\tilde{Q}_k=Q_k-\Delta Q_k;\\
&\tilde{\lambda}_k=\lambda_k-\Delta\lambda_k;\\
&\tilde{R}_k=R_k-\Delta R_k;\\
&\tilde{M}_k=M_k-\Delta M_k.
\end{aligned} \qquad (5)$$

Здесь значок ~ обозначает точное значение, а Δ – случайную ошибку.

Наложим на рассматриваемую систему стандартные условия управляемости и наблюдаемости [8]:

матрица управляемости $C(k,j)\triangleq\sum_{i=j}^{k}\phi(k,i+1)Q_i\phi^T(k,i+1),\ j\le k$, долж-

на иметь ранг, равный n:

$$rank\ C(k,j) = n; \quad (6)$$

матрица наблюдаемости $S(k,j) \triangleq \sum_{i=j}^{k} \phi^T(i,k) M_i^T R_i^{-1} M_i \phi^T(i,k),\ j \le k$, должна иметь ранг, равный n:

$$rank\ S(k,j) = n. \quad (7)$$

Кроме того, мажорируем переходную матрицу некоторой экспоненциальной функцией:

$$\|\phi(k,1)\| \le a e^{-b(k-1)} \quad \forall k, \quad (8)$$

где a, b – положительные константы, определяемые параметрами системы идентификации.

Система управления, для которой выполняются условия (6–8), является равномерно асимптотически устойчивой. Для такой системы среднее значение ошибки оценки вектора X_k, определяемое уравнением вида

$$m(k/k-1) \triangleq E[X_k] - E\left[\tilde{X}(k/k-1)\right] = E\left[X_k - \tilde{X}(k/k-1)\right], \quad (9)$$

асимптотически стремится к нулю при $k \to \infty$. Другими словами, для алгоритма оценивания (3) при положительно определенной матрице $P(0/0)$ влияние начальных условий экспоненциально ослабевает по мере поступления новых результатов измерений. Следовательно, априорное математическое ожидание $m(0/0)$ в начальный момент времени может быть отличным от нуля.

Соответственно дисперсия ошибок оценивания также асимптотически стремится к нулю, а время корреляции ошибок невелико по сравнению с длительностью интервала наблюдения. Следовательно, фильтр, с помощью которого реализуется алгоритм идентификации, может иметь конечную память (конечную импульсную характеристику).

Рассмотрим поведение невязок измерений, вектор которых определяется из четвертого уравнения алгоритма (3). Матрица ковариаций невязки измерений в k-й момент времени при неточном определении матриц $M_k, P(k/k-1), R_k$ равна по определению

$$P(\nu_k) \triangleq M_k P(k/k-1) M_k^T + R_k. \quad (10)$$

При точных значениях данных матриц

$$\tilde{P}(\nu_k) \triangleq E\left[\nu_k \nu_k^T\right] - \tilde{\nu}_k \tilde{\nu}_k^T, \quad (11)$$

где

$$\tilde{\nu}_k \triangleq E[\nu_k] = M_k m(k/k-1) - \Delta M_k. \quad (12)$$

С учетом условия (8) и уравнения (9) запишем выражение для эволюции ошибки оценки

$$\Delta P_k = \tilde{P}(\nu_k) - E\left[P(\nu_k)\right],\ k = 1,2,3,\ldots:$$

$$\left|\Delta P(\nu_k)\right| = \left| E\left[\nu_k \nu_k^T\right] - \tilde{\nu}_k \tilde{\nu}_k^T - E\left[M_k P k/k-1 M_k^T + R_k\right] \right| \le a_\nu e^{-b_\nu [k-1]} \quad (13)$$

Откуда

$$\lim_{k \to \infty} \|\Delta P(\nu_k)\| \to 0. \quad (14)$$

Здесь a_ν, b_ν – положительные константы. Таким образом, для равномерно асимптотически устойчивого алгоритма (3) при выполнении условий (6–8) невязки измерений экспоненциально стремятся к нулю.

Используя выражения (6–14), теоретически можно идентифицировать матрицы $\tilde{\Phi}$, $\tilde{\lambda}$, $\tilde{Q}$, $\tilde{R}$ с требуемой точностью за конечное число шагов. Однако для практической реализации алгоритма идентификации необходимо находить условия равенства нулю математического ожидания некоторых функций от этих матриц как случайных функций времени. Рассмотрим векторную функцию

$\vec{F}\left(\vartheta_k, \vec{\gamma}\right)$, где матрица ϑ_k - одна из матриц $\phi_k, \lambda_k, Q_k, R_k$ в уравнениях (5); $\vec{\gamma}$ – вектор случайных параметров. Это могут быть невязки измерений ν_k или/и шумы измерений η_k. Для опре-деления $\vec{\gamma}$ необходимо решать уравнение вида

$$m\left(\vec{\gamma}\right) \triangleq E\left[\vec{F}\left(\vartheta_k, \vec{\gamma}\right)\right] = 0 \quad . \quad (15)$$

В общем случае $\vec{F}\left(\vartheta_k, \vec{\gamma}\right)$ является случайной функцией произвольного вида, поэтому точное решение уравнений вида (15) практически невозможно. Наиболее простыми и эффективными методами приближенного решения являются поисковые методы, основанные на стохастической аппроксимации [9] математического ожидания $m\left(\vec{\gamma}\right)$ его текущей реализацией $\vec{\gamma}_n$. Для вычисления используется рекуррентное уравнение вида

$$\vec{\gamma}_{n+1} = \vec{\gamma}_n - \beta_n \left\{ E\left[\nabla \vec{F}\left(\vartheta_n, \vec{\gamma}_n \right) \right] \right\}^{-1} , \quad (16)$$

где β_n – величина шага n-й итерации в направлении статистического антиградиента функции $\vec{F}\left(\vartheta_n, \vec{\gamma}_n \right)$. По существу, уравнение (16) представляет собой статистический аналог градиентного метода поиска экстремума многомерной функции.

Выбор функции изменения шага β_n зависит от многих факторов, в первую очередь – от вида минимизируемой функции Простейший выбор: $\beta_n = \beta_0 / n$, где β_0 – шаг на начальной итерации.

Выводы

1. Пошаговая идентификация параметров и состояния сети на основе дискретного фильтра Калмана, по существу, сводится к решению задачи оценивания корреляционной матрицы и переходной матрицы состояния системы.

2. Для сложных систем достаточно высокого порядка, состоящих из множества слабо связанных между собой объектов, задача глобальной идентификации распадается на совокупность частных задач идентификации низкого порядка.

Список литературы

1. *Віноградов М.А.* Особливості охорони об'єктів зв'язку категорії Б – лінійне обладнання / [Віноградов М.А., Коробко В.В., Скоропаденко О.П. та ін.] // Зв'язок. – 2004. – № 4. – С. 38-41.

2. *Виноградов Н.А.* Анализ потенциальных характеристик устройств коммутации и управления сетями новых поколений / Н.А. Виноградов // Зв'язок. – 2004. – №4. – С. 10-17.

3. *Вентцель Е.С.* Исследование операций / Е.С. Вентцель – М.: Советское радио, 1972. – 552 с.

4. *Казаков И.Е.* Статистическая динамика систем с переменной структурой / И.Е. Казаков– М.: Наука, 1977. – 416 с.

5. *Kalman R.E.* A new approach to linear filtering and predicting problems / R.E. Kal-man // Transaction of American Society of Mechanic Engineers, Series D, Journal of Ba-sic Engineering. – 1960. – v. 82. – P. 35-45.

6. *Балакришнан А.В.* Теория фильтрации Калмана / А.В. Балакришнан– М.: Мир, 1988. – 168 с.

7. *Сейдж Э.* Теория оценивания и ее применение в связи и управлении / Э. Сейдж, Дж. Мелс; под ред. проф. Б.Р. Левина. – М.: Связь, 1976. – 496 с.

8. *Воронов А.А.* Устойчивость, управляемость, наблюдаемость / А.А. Воронов – М.: Наука, 1979. – 336 с.

9. *Аоки М.* Введение в методы оптимизации / М. Аоки– М.: Наука, 1977. – 344 с.

Подано до редакції 16.12.2010