Expert SystemsInformation ClassificationAnalysis for Enterprise Communication Networks Security Estimation

Olga Poluektova

Information Security Department, Lviv Polytechnic National University, UKRAINE, Lviv, S. Banderystreet 12,
E-mail: poluektova.ol@gmail.com

In paper the algorithm of dynamic classification analysis are suggested for the treatment of information, what the expert system gets.

The topology of physical and logical connections of corporate networks with every year is complicated, loading on a network is rised, the new methods of violation are appear. All of these factors determine a necessity for creation of the system which can analyse the protection of corporate communication networks and can accept independent decisions in relation to the removal of negative influence of factors.

The information about corporate communication network protection is dynamic; knowledge about a subject domain can change in time of the decision-making. Therefore the problem of analysis of much-self-reactance dynamic information was appeared. It is impossible to use the ordinary algorithms of automatic classification when we research information which changes dynamically. The special algorithms of dynamic classification analysis were developed.

For the treatment of entrance information dynamic classification analysiscan be offered, when every object on an every parameter was characterized of the set of values for some sequence of moments of the time.

The theoretical analysis of this algorithm shows that optimum classification can be searched in the narrow class of standard classifications and it is determined the gradient of initial functional (criterion of quality).

The task of the dynamic classification analysis is formulated with the use of three basic concepts: plural of objects, that were classified, class of possible classifications and functional of quality of laying out.

In paper were proposed to build the criterion of quality of classifications in accordance with a method of the generalized middle and to classify the eventual plural of obektiv, which change dinamically.

Класифікаційний аналіз інформації в експертних системах для оцінки захищеності корпоративних мереж зв'язку

Ольга Полуектова

Кафедра захисту інформації, Національний університет "Львівська політехніка", УКРАЇНА, м.Львів, вул.С.Бандери, 12,
E-mail: poluektova.ol@gmail.com

В роботі запропоновано застосовувати алгоритм динамічного класифікаційного аналізу як інструмент обробки інформації, що отримується експертною системою для оцінки захищеності корпоративних мереж зв'язку (КМЗ).

Ключові слова – корпоративна мережа зв'язку, експертна система, алгоритм динамічного класифікаційного аналізу, множина об'єктів.

Вступ

Топологія фізичних та логічних зв'язків корпоративних мереж з кожним роком ускладнюється, підвищується навантаження на мережі, з'являються нові методи порушення роботи, що можуть обмежувати доступ законних власників до даних та порушувати цілісність інформації. Всі ці фактори визначають необхідність у створенні системи, що може аналізувати стан захищеності корпоративних мереж зв'язку (КМЗ) та приймати самостійні рішення щодо усунення негативного впливу факторів. Такою системою може стати експертна система для оцінки захищеності КМЗ.

Оскільки інформація про стан захищеності КМЗє динамічною, знання про предметну область можуть змінюватись за час вирішення задачіпостає проблема аналізу багатопараметричної динамічної інформації. Безпосереднє використання класичних методів аналізу (емпіричних, логічних, евристичних) в такій ситуації неможливе. Для обробки вхідної інформації можна запропонувати динамічний класифікаційний аналіз (ДКА), коли кожен об'єкт за кожним параметром характеризується набором значень для деякої послідовності моментів часу (траєкторій). Під об'єктом розуміємо складову КМЗ, окрему службу персонального комп'ютера, тощо.

II. Методи структуризації динамічних об'єктів

При дослідженні багатопараметричної інформації, що динамічно змінюється, неможливо використовувати звичайні алгоритми автоматичної класифікації. Були розроблені спеціальні алгоритми динамічного класифікаційного аналізу (ДКА), коли кожен об'єкт по кожному параметру характеризується набором значень для деякої послідовності моментів часу

(траєкторій). В рамках варіаційного підходу розроблений відповідний алгоритм ДКА. Теоретичний аналіз [1] цього алгоритму показує, що оптимальну класифікацію можна шукати у вузькому класі еталонних класифікацій, і вона визначається градієнтом вихідного функціонала (критерія якості).

Постановка задачі ДКА формулюється з використанням трьох основних понять: множина об'єктів, що класифікуються, клас допустимих класифікацій та функціонал якості розбиття.

1) Множина об'єктів, що класифікуються

В ДКА пропонується класифікувати кінцеву множину об'єктів, які динамічно змінюються. Нехай в кожен момент часу об'єкти описуються деяким конкретним набором параметрів $x^{(1.1)},...,x^{(k)}$. Вважається, що для кожного об'єкта послідовно фіксуються m значень кожного із параметрів у відповідні моменти часу. Тому, кожен об'єкт характеризується серією із m векторів $x_1,...,x_m$ в k-вимірному просторі параметрів, що є траєкторією зміни даного об'єкта в просторі параметрів. Таку траєкторію позначають через $\tilde{x} = (x_1,...,x_m)$. В якості сукупності об'єктів розглядається кінцева множина об'єктів, що задається своїми траєкторіями фіксованої довжини, тобто необхідно класифікувати множину $X = \{\tilde{x}_1,...,\tilde{x}_n\}(X \subseteq R^{k*m})$. Особливість такого підходу в тому, що моменти часу, в які зафіксовані значення параметрів, у різних об'єктів можуть бути різними.

2) Клас допустимих класифікацій

Нечіткою класифікацією множини $X = \{\tilde{x}_1,...,\tilde{x}_n\}$ на r класів з фоновим класом називається $(r+1)$-вимірнавектор-функція (1):

$$H(\tilde{x}) = (h_0(\tilde{x}), h_1(\tilde{x}),..., h_r(\tilde{x})) \qquad (1)$$

У виразі (1) $h_0(\tilde{x})$ функція належності $\tilde{x}$ до фонового класу, а $h_i(\tilde{x})$ функція його приналежності до i-го класу. Для будь-якого $\tilde{x}$ значення $H(\tilde{x})$ повинна належати деякій обмеженій замкнутій множині V простору значень вектор-функції H, тобто $H(\tilde{x}) \in V \subseteq R^{r+1}$. Множина V визначає тип нечіткості для даної задачі. Тому, розглядається такий клас нечітких класифікацій (2):

$$\Xi(V) = \left\{ H : \forall \tilde{x} \in X \quad H(\tilde{x}) \in V \right\} \qquad (2)$$

3) Критерій якості класифікацій

Для ДКА пропонується будувати критерій якості класифікацій у відповідності з методом узагальненого середнього. Вважається, що об'єкти одного і того ж класу класифікації повинні добре описуватися деякою моделлю траєкторії цього класу, а об'єкти, чиї траєкторії погано описуються всіма моделями класів, повинні попасти в фоновий клас [1]. Тому критерій якості повинен відображати:

- близькість траєкторії об'єктів всередині нефонових класів;
- віднесення до фонового класу об'єктів, чиї траєкторії достатньо віддалені від моделей нефонових класів [2].

Необхідно розглянути множину Λ можливих моделей траєкторії класів. Між елементами множини об'єктів X і елементами множини моделей Λ вводиться міра близькості $K(\tilde{x},\tilde{a})(\tilde{x} \in X; \tilde{a} \in \Lambda)$.

Величина (3):

$$K(h(\tilde{x}),\tilde{a}) = \sum_{j=1}^{n} K(\tilde{x}_j,\tilde{a}) h(\tilde{x}_j) \qquad (3)$$

відображає міру того, наскільки добре модель $\tilde{a}$ описує точки множини, що задана через свою функцію належності $h(\tilde{x})$.

Узагальненим середнім або еталоном множини, що задана функцією належності $h(\tilde{x})$, називається модель (4):

$$\tilde{a}_h = \arg\max_{\tilde{a} \in \Lambda} K(h(\tilde{x}),\tilde{a}) \qquad (4)$$

Відповідно до (4) вводиться такі критерій якості класифікації (5):

$$J(H) = \sum_{i=1}^{n} K(h_i(\tilde{x}),\tilde{a}_{h_i}) + B\sum_{i=1}^{n} h_0(\tilde{x}_j), \qquad (5)$$

де $\tilde{a}_{h_i}$ еталон i-го класу (), а B – деяка константа, яка визначає який об'єкт можна віднести до фонового класу.

Задача класифікації полягає в максимізації функціонала (5) по вектор-функціям належності об'єктів до класів H. Крім того, в кожному класі є еталонна траєкторія, що відображає загальну тенденцію зміни значень показників для об'єктів даного класу [1].

Висновок

Описана методика динамічного класифікаційного аналізу складно-організованої інформації використовується для зменшення надлишковості та структуризації інформації при аналізі та наповненні бази знань експертної системи для оцінки захищеності корпоративної мережі зв'язку.

Література

[1] Покровская И.В. Экспертно-классификационный анализ данных в задаче оценки эффективности функционирования крупномасштабных систем управления / И.В Покровская., М.Д. Гольдовская, Ю.А Дорофеюк // Таврический вестник информатики и математики. – Симферополь, 2008 - №2. – С. 159-165.

[2] Дорофеюк Ю.А. Методы структурно-классификационного прогнозирования многомерных динамических обьектов / Ю.А. Дорофеюк, А.А. Дорофеюк // «Искусственный интеллект» 2. – Киев 2006. – С. 138-141.