PRZEGLĄD TELEINFORMATYCZNY
NR 1-2, 2018

Wykrywanie anomalii bazujące na wskazanych przykładach

Włodzimierz KWIATKOWSKI

Instytut Teleinformatyki i Automatyki, Wydział Cybernetyki, WAT,
ul. Gen. W. Urbanowicza 2, 00-908 Warszawa 46
wlodzimierz.kwiatkowski@wat.edu.pl

STRESZCZENIE: Rozpatrywany jest problem wykrywania anomalii na podstawie zarejestrowanych obserwacji zachowania systemu. Problem jest sformułowany jako zadanie rozpoznawania wzorców zachowania normalnego i zachowania nietypowego. Obydwa wzorce są określane przez wskazanie odpowiednich przykładów. Osobliwość rozwiązywanego zadania wynika z faktu, że zwykle liczebność przykładów jest dużo mniejsza od wymiaru wektora obserwacji. W artykule zostały przedstawione dwie metody detekcji anomalii bazujące na wyznaczaniu rzutów obserwacji na podprzestrzenie wzorców. Wyróżnikiem pierwszej metody jest wykorzystywanie odległości wektora obserwacji od podprzestrzeni wzorców. Druga metoda polega na przeniesieniu zadania rozpoznawania wzorców do podprzestrzeni wzorców.

SŁOWA KLUCZOWE: wykrywanie anomalii, rozpoznawanie wzorców, eksploracja danych, odległość Mahalanobisa

1. Wprowadzenie

Wykrywanie anomalii (nieprawidłowości) należy do podstawowych problemów administrowania systemami, w tym komputerowymi i teleinformatycznymi. Jest to także zasadniczy problem szeroko rozumianej diagnostyki (m.in. technicznej, medycznej). Wykrywanie anomalii nie jest jednak tożsame z testowaniem systemu. Celem testowania systemu jest wykrywanie błędów w systemie i sprawdzenie jego wymaganej funkcjonalności. Przykładem może być testowanie (weryfikacja, walidacja) oprogramowania. Testowanie systemu ma zwykle charakter interaktywny. Polega to na podawaniu do systemu określonych wymuszeń i porównywaniu uzyskiwanej reakcji systemu z reakcją oczekiwaną, zwykle wcześniej określoną w dokumentacji systemu. Wykrywanie

anomalii ma charakter pasywny i jej celem jest sprawdzenie czy zachowanie systemu nie zmieniło się w stosunku do jego normalnej pracy.

Najczęściej wykrycie anomalii sprowadza się do stwierdzenia niezgodności obserwacji z modelem (regułami) działania systemu. Takie podejście obejmuje więc przypadki zaobserwowania wartości odstających (*outliers*, *discordant observations*), wyjątków (*exceptions*), osobliwości (*peculiarities*) czy też po prostu nowych zachowań (*novelty items*). Konsekwencją stwierdzenia anomalii może być konieczność odstąpienia od zarządzania (sterowania) bazującego na wykorzystywanym modelu (i np. przejście do procedury obsługi wyjątków). Zaobserwowanie wartości odstających zwykle skutkuje nieuwzględnianiem ich w formułowaniu modelu działania systemu. Pozostałe przypadki wymagają najczęściej modyfikacji lub zmiany modelu.

Wykrywanie anomalii wymaga uprzedniego określenia, jakie obserwacje (pomiary, cechy) będą podstawą wnioskowania. Od trafności przyjętych ustaleń zależy użyteczność orzeczeń.

Wykrycie anomalii z reguły następuje w wyniku weryfikacji hipotezy „zachowanie jest normalne". Takie podejście wymaga zdefiniowania specjalnego modelu normalności. Model ten jest rozumiany jako zestaw reguł do orzeczenia zgodności obserwacji z przyjętym modelem działania systemu. W szczególnym przypadku budowa takiego modelu może polegać na wyznaczeniu obszaru normalności w przestrzeni obserwacji (pomiarów, cech).

Weryfikacja hipotezy „zachowanie jest normalne" przeciwko alternatywnej hipotezie złożonej „zachowanie nie jest normalne" jest zdecydowanie trudniejsza niż w przypadku, gdy hipoteza alternatywna jest prosta (np. „zachowanie nie jest normalne z powodu awarii podzespołu A"). W drugim przypadku problem zostaje zawężony do wykrywania interesującej nas anomalii (nieprawidłowości). Nie można jednak oczekiwać, że uda się skatalogować wszystkie przypadki anomalii i opracować dla nich odpowiednie alternatywne hipotezy proste. Poszukuje się więc rozwiązań kompromisowych między wnioskowaniem na podstawie znanego modelu normalności bez żadnej wiedzy o anomaliach, a wnioskowaniem na podstawie znanego modelu normalności i znanego modelu anomalii. Kompromis ten można osiągnąć wskazując zaobserwowane przykłady (przypadki) zachowań zarówno normalnych, jak i anomalnych (*anomalous*).

Przegląd metod rozwiązywania problemu wykrywania anomalii jest przedstawiony w [5]. Przyjęte w [2] sformułowanie problemu wykrywania anomalii obejmuje jako przypadki szczególne wykrywanie nowych zachowań (*novelty detection*) [6] oraz wykrywanie zachowań odstających (*outliers*) [3]. W tych szczególnych przypadkach wymagane jest określenie jedynie wzorca normalności, a zachowanie z nim niezgodne można określić jako anormalne (*abnormal*). Problem wykrywania zachowań anormalnych pojawia się

w przypadku analizy obserwacji nieoznakowanych (*unsupervised outlier detection*) [1, 9].

2. Wykrywania anomalii na podstawie przykładów

W niniejszym artykule zadanie wykrywania anomalii jest formułowane jako zadanie rozpoznawania wzorców: normalności i anomalii. Sformułowanie tego zadania jest z natury rzeczy trudne. Model statystyczny zachowania normalnego może okazać się zbyt ogólny i z tego powodu wnioskowanie bazujące na ocenie zgodności z nim obserwacji (danych) może być zawodne [2].

Podstawowa trudność budowy modelu anomalii wynika z faktu, że nie jest z góry wiadome, jaki rodzaj obserwacji (danych) może ujawnić odstępstwa od stosowanego modelu. Z tego powodu do wykrywania anomalii próbuje się wykorzystywać wszystkie dostępne dane, choćby tylko potencjalnie użyteczne. Takie podejście prowadzi do konieczności analizy zbiorów danych charakteryzujących się dużymi rozmiarami i dużą rozmaitością. Dane tego typu są uzyskiwane przy automatycznym dokumentowaniu różnorodnych działań (*digital footprint*, *digital shadow*). Model generowania tych danych zwykle nie jest znany.

W tej sytuacji stosowanie analizy typu potwierdzającego (*confirmatory data analysis*) i bazującej na modelach statystycznych jest kontestowane [2]. Alternatywą są badania o charakterze wydobywczym, powszechnie określane jako eksploracja danych (*exploratory data analysis*) [7]. Rutynową techniką wykorzystywaną w eksploracyjnej analizie danych do selekcji wyników obserwacji jest analiza głównych składowych (*principal component analysis*, PCA). W szczególności umożliwia ona redukcję liczby współrzędnych wektora obserwacji.

Rozpatrywany w niniejszym artykule problem dotyczy typowej w zadaniach wykrywania anomalii sytuacji, gdy liczba wskazanych przykładów wzorców (zwłaszcza wzorców anomalii) jest mała względem liczby współrzędnych wektora wyników obserwacji. Wtedy przy analizie obserwacji wzorcowych przypadków występują składowe główne, które charakteryzują się zerową wariancją. Z formalnego punktu widzenia celem przedstawianych dalej badań jest uzyskanie metod minimalnoodległościowych rozpoznawania wzorców wtedy, gdy wymiar przestrzeni obserwacji jest większy od wymiaru podprzestrzeni generowanej przez składowe główne o niezerowej wariancji.

3. Przestrzeń wyników obserwacji

Podstawą badań są wyniki obserwacji zachowań analizowanej klasy systemów. Każda obserwacja odnosi się do jednego przykładu zachowania sytemu. Wynikiem każdej obserwacji jest wektor złożony z ustalonej liczby współrzędnych (interpretowanych jako cechy zachowania systemu). Omawiane wyniki są zestawiane w postaci następującej macierzy:

$$\mathbf{W} = \left[\mathbf{w}_1,\ \mathbf{w}_2,\ \ldots\ \mathbf{w}_N\right] \tag{1}$$

gdzie:

$$\mathbf{w}_k = \begin{bmatrix} w_{1,k} \\ w_{2,k} \\ \ldots \\ w_{L,k} \end{bmatrix} \tag{2}$$

Parametr N oznacza liczbę wszystkich przykładów zachowań, a parametr L – liczbę współrzędnych wektora obserwacji. Oznaczymy dalej macierz kowariancji obserwacji następująco:

$$\mathbf{R} = \tfrac{1}{N-1}\sum_{k=1}^{N}\left(\mathbf{w}_k - \overline{\mathbf{w}}\right)\left(\mathbf{w}_k - \overline{\mathbf{w}}\right)^T \tag{3}$$

gdzie:

$$\overline{\mathbf{w}} = \tfrac{1}{N}\sum_{k=1}^{N}\mathbf{w}_k \tag{4}$$

Przyjmiemy dalej, że

$$rank\left(\mathbf{R}\right) = L \tag{5}$$

Odległość pomiędzy wektorami $\mathbf{x}$, $\mathbf{y}$ przestrzeni cech R^L będziemy wyznaczać w sposób uwzględniający wielkość rozrzutu (rozproszenia) współrzędnych pomiaru oraz ich wzajemną korelację. Wymaganie to spełnia odległość Mahalanobisa określona wzorem:

$$\mathrm{d}(\mathbf{x},\mathbf{y}) = \sqrt{(\mathbf{x}-\mathbf{y})^T\,\mathbf{R}^{-1}(\mathbf{x}-\mathbf{y})}\,, \qquad \mathbf{x},\mathbf{y} \in R^L \tag{6}$$

4. Rozpoznawanie wzorców metodą minimalnej odległości

Wskazania przykładów obserwacji zakwalifikowanych do wzorca o indeksie $h \in \{1,2,\ldots,H\}$ (gdzie: H – liczba wzorców) będziemy dokonywać przez podanie odpowiedniego zbioru indeksów W_h. Rozpatrywany wzorzec będzie więc reprezentowany przez następujący zbiór punktów (klaster) w przestrzeni obserwacji:

$$C(W_h) = \{\mathbf{w}_k : k \in W_h\} \tag{7}$$

składający się ze wskazanych przykładów obserwacji. Liczbę elementów tak rozumianego wzorca W_h oznaczymy jako $N_h = \|C(W_h)\|$. Wnioskowanie o podobieństwie obserwacji $\mathbf{x}$ do wzorca W_h bazuje na określeniu odległości punktu $\mathbf{x}$ od klastra $C(W_h)$. Przykładowo, wybierając metodę centroidalną wyznaczania odległości między klastrami, otrzymujemy zależność:

$$\mathrm{D}(\mathbf{x}, C(W_h)) = \mathrm{d}(\mathbf{x}, \overline{\mathbf{w}}_h) = \sqrt{(\mathbf{x} - \overline{\mathbf{w}}_h)^T \mathbf{R}^{-1} (\mathbf{x} - \overline{\mathbf{w}}_h)} \tag{8}$$

gdzie:

$$\overline{\mathbf{w}}_h = \tfrac{1}{N_h} \sum_{j \in W_h} \mathbf{w}_j \tag{9}$$

Z uwagi na sposób wyznaczenia macierzy kowariancji $\mathbf{R}$ taka metoda wnioskowania znajduje uzasadnienie tylko wtedy, gdy pomiary odpowiadające wszystkim wzorcom są jednorodne w następującym sensie: odpowiednie klastry różnią się jedynie wartościami oczekiwanymi (a odpowiadające im macierze kowariancji są jednakowe).

W wielu zagadnieniach, a zwłaszcza w przypadku badania anomalii macierze kowariancji wzorców różnią się. Rozpatruje się wtedy możliwość zróżnicowania sposobu pomiaru odległości stosownie do macierzy kowariancji poszczególnych wzorców [4].

Macierz kowariancji wyznaczoną na podstawie przykładów wzorca W_h oznaczymy następująco:

$$\mathbf{R}_h = \tfrac{1}{N_h - 1} \sum_{j \in W_h} \left(\mathbf{w}_j - \overline{\mathbf{w}}_h\right)\left(\mathbf{w}_j - \overline{\mathbf{w}}_h\right)^T \tag{10}$$

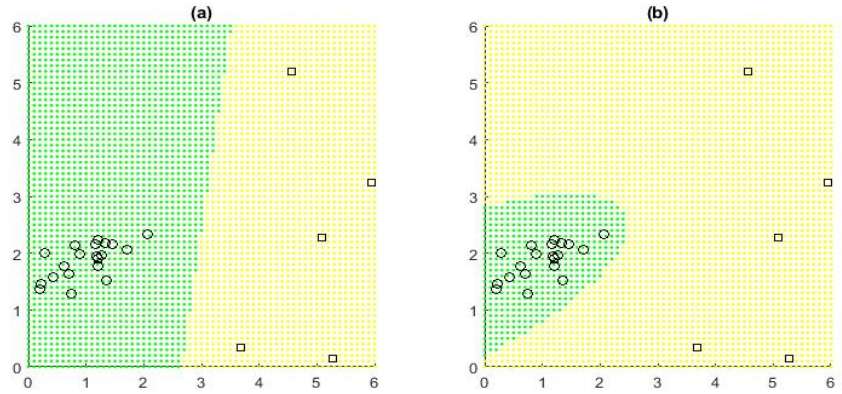
Odległość pomiędzy wektorami $\mathbf{x}$, $\mathbf{y}$ przestrzeni cech R^L zadaną wzorem:

$$\mathrm{d}_h(\mathbf{x}, \mathbf{y}) = \sqrt{(\mathbf{x} - \mathbf{y})^T \mathbf{R}_h^{-1} (\mathbf{x} - \mathbf{y})}, \qquad \mathbf{x}, \mathbf{y} \in R^L \tag{11}$$

nazywać będziemy dopasowaną do wzorca W_h. Podobnie nazywać będziemy odległość między obserwacją $\mathbf{x}$ a klastrem $C(W_h)$. Przykładowo dla metody centroidalnej odległość ta jest określona wzorem:

$$D_h(\mathbf{x}, C(W_h)) = \mathrm{d}_h(\mathbf{x}, \overline{\mathbf{w}}_h) = \sqrt{(\mathbf{x} - \overline{\mathbf{w}}_h)^T \mathbf{R}_h^{-1} (\mathbf{x} - \overline{\mathbf{w}}_h)} \tag{12}$$

Na rys. 1 przedstawiony jest przykład ilustrujący różnice powodowane wykorzystywaniem odległości dopasowanych do poszczególnych wzorców: W_1 bądź W_2. Punkty przykładów wzorcowych $C(W_1)$ są przedstawionych na rysunku jako kółka, punkty przykładów wzorcowych $C(W_2)$ – jako kwadraty. Punkty przestrzeni obserwacji leżące bliżej przykładów wzorcowych $C(W_1)$ są oznaczone kolorem ciemniejszym. Przedstawiona na rys.1(a) metoda klasyfikacji prowadzi do uzyskania wyników analogicznych do otrzymywanych w liniowej analizie dyskryminacyjnej (LDA, *linear discriminant analysis*). Rozwiązanie przedstawione na rys. 1(b) ma bezpośrednie odniesienie do kwadratowej analizy dyskryminacyjnej (QDA, *quadratic discriminant analysis*).



Rys. 1.
(a) Do wyznaczania odległości wykorzystywane są metryki bazujące na macierzy kowariancji obliczonej dla wszystkich obserwacji razem, zgodnie z wzorem (6).
(b) Do wyznaczania odległości wykorzystywane są metryki bazujące na macierzy kowariancji obliczanych dla obserwacji każdego wzorca osobno, zgodnie z wzorem (11).

5. Podprzestrzeń wzorca W_h

Jeśli macierz $\mathbf{R}_h$ jest osobliwa, obliczenie odległości dopasowanej (12) jest niemożliwe. W takim przypadku proponujemy zredukować liczbę współrzędnych pomiarów tak, aby w uzyskanej w ten sposób podprzestrzeni odpowiednia macierz kowariancji była nieosobliwa. Podprzestrzeń uzyskaną w ten sposób nazywać będziemy podprzestrzenią wzorca W_h.

Proponujemy dalej, aby redukcję wymiaru wektora pomiaru przeprowadzić w przestrzeni wartości transformat Karhunena-Loève'a [4]. Podstawą przekształcenia Karhunena-Loève'a są ortonormalne wektory własne $\mathbf{t}_k(\mathbf{R}_h)$ macierzy kowariancji $\mathbf{R}_h$. Wektory te spełniają następującą zależność:

$$\mathbf{R}_h\,\mathbf{t}_k(\mathbf{R}_h) = \lambda_k(\mathbf{R}_h)\mathbf{t}_k(\mathbf{R}_h), \qquad k = 1,2,\cdots,L \tag{13}$$

gdzie: $\mathbf{t}_k(\mathbf{R}_h) = \begin{bmatrix} t_{k,1} \\ t_{k,2} \\ \cdots \\ t_{k,L} \end{bmatrix}$. a $\lambda_k(\mathbf{R}_h)$ – wartości własne macierzy kowariancji $\mathbf{R}_h$.

Wartości własne $\lambda_k(\mathbf{R}_h)$ są liczbami rzeczywistymi; przyjmujemy, że wartości te są uporządkowane malejąco względem indeksu k. Wtedy macierz przekształcenia Karhunena-Loève'a można przedstawić następująco:

$$\mathbf{T}_h = \begin{bmatrix} \mathbf{t}_1^T(\mathbf{R}_h) \\ \mathbf{t}_2^T(\mathbf{R}_h) \\ \cdots \\ \mathbf{t}_L^T(\mathbf{R}_h) \end{bmatrix} \tag{14}$$

Transformaty różnic $\mathbf{w}_k - \overline{\mathbf{w}}_h$ oznaczymy następująco:

$$\mathbf{v}_k = \mathbf{T}_h(\mathbf{w}_k - \overline{\mathbf{w}}_h), \qquad k \in W_h \tag{15}$$

gdzie $\overline{\mathbf{w}}_h$ jest określone wzorem (9). Macierz kowariancji $\mathbf{V}_h$ wektorów $\mathbf{v}_k$ jest macierzą diagonalną:

$$\mathbf{V}_h = \tfrac{1}{N_h - 1}\sum_{k=1}^{N_h}\left(\mathbf{v}_k - \overline{\mathbf{v}}_h\right)\left(\mathbf{v}_k - \overline{\mathbf{v}}_h\right)^T = diag\left(\lambda_1(\mathbf{R}_h), \lambda_2(\mathbf{R}_h), \ldots, \lambda_L(\mathbf{R}_h)\right) \tag{16}$$

przy czym: $\overline{\mathbf{v}}_h = \tfrac{1}{N_h}\sum_{k=1}^{N_h}\mathbf{v}_k = \mathbf{0}$.

Niech $M_h \le \min\{N_h, L\}$ oznacza liczbę dodatnich wartości własnych macierzy kowariancji $\mathbf{R}_h$. Niech wektory $\boldsymbol{v}_k$ podprzestrzeni R^{M_h} będą wyznaczone na podstawie wektorów $\mathbf{v}_k$ przestrzeni R^L w następujący sposób:

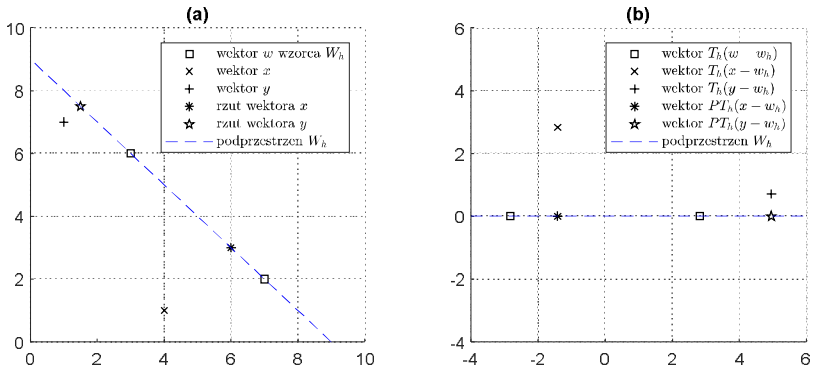
$$\boldsymbol{v}_k = \mathbf{P}\mathbf{v}_k = \begin{bmatrix} 1 & \cdots & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & & 0 & \cdots & 0 \end{bmatrix} \begin{bmatrix} v_{k,1} \\ \cdots \\ v_{k,M_h} \\ \cdots \\ v_{k,L} \end{bmatrix} = \begin{bmatrix} v_{k,1} \\ v_{k,2} \\ \cdots \\ v_{k,M_h} \end{bmatrix}, \qquad k \in W_h \tag{17}$$

Macierz kowariancji $\mathbf{Q}_h$ uzyskanych w ten sposób wektorów $\boldsymbol{v}_k$ jest następująca:

$$\mathbf{Q}_h = diag\left(\lambda_1(\mathbf{R}_h), \lambda_2(\mathbf{R}_h), \ldots, \lambda_{M_h}(\mathbf{R}_h)\right) \tag{18}$$

Macierz ta, zgodnie z uczynionym założeniem, jest dodatnio określona. Odległość Mahalanobisa wektorów $\boldsymbol{x}$, $\boldsymbol{y}$ podprzestrzeni R^{M_h} zdefiniujemy następująco:

$$d_h(\boldsymbol{x}, \boldsymbol{y}) = \sqrt{(\boldsymbol{x}-\boldsymbol{y})^T \mathbf{Q}_h^{-1} (\boldsymbol{x}-\boldsymbol{y})} \tag{19}$$



Rys. 2. (a) Rzutowanie w przestrzeni obserwacji. (b) Rzutowanie w przestrzeni transformat Karhunena-Loève'a.

Ilustracja odwzorowania wektorów przestrzeni cech R^{N_h} w wektory podprzestrzeni transformat R^{M_h} została przedstawiona na rys. 2 (w rozpatrywanym przykładzie $L = N_h = 2$, $M_h = 1$). Wektory obserwacji $\mathbf{x}$, $\mathbf{y}$ należą do

przestrzeni R^2. Przestrzeń transformat jest także dwuwymiarowa, wektory $\mathbf{T}_h\mathbf{x}$, $\mathbf{T}_h\mathbf{y}$ należą do tej przestrzeni. Podprzestrzeń wzorca W_h jest jednowymiarowa: $R^{M_h} = R^1$. Wektory $\mathbf{PT}_h(\mathbf{x} - \overline{\mathbf{w}}_h)$, $\mathbf{PT}_h(\mathbf{y} - \overline{\mathbf{w}}_h)$ są wynikiem rzutowania $\mathbf{P}$ wektorów $\mathbf{T}_h(\mathbf{x} - \overline{\mathbf{w}}_h)$, $\mathbf{T}_h(\mathbf{y} - \overline{\mathbf{w}}_h)$ na podprzestrzeń $R^{M_h} = R^1$.

6. Metryki dopasowane do wzorca W_h

W niniejszym punkcie proponujemy rozwiązanie problemu oceny stopnia podobieństwa wektora $\mathbf{x}$ przestrzeni obserwacji R^L do wzorca W_h. Rozwiązanie to bazuje na wyznaczonej wcześniej podprzestrzeni wzorca. Podstawą naszych propozycji są dwie metody wyznaczania odległości dopasowanej do wzorca W_h.

6.1. Metoda rzutowania na podprzestrzeń wzorca

Dopasowaną do wzorca W_h odległość między pomiędzy wektorami $\mathbf{x}$, $\mathbf{y}$ przestrzeni cech R^L proponujemy wyznaczać jako odległość między rzutami tych wektorów na podprzestrzeń wzorca. Biorąc pod uwagę fakt, że transformacja $\mathbf{T}_h$ Karhunena-Loève'a jest przekształceniem ortogonalnym, odpowiednie obliczenia można wykonać w przestrzeni transformat. Po wyznaczeniu rzutów $\boldsymbol{x}_h = \mathbf{PT}_h\mathbf{x}$, $\boldsymbol{y}_h = \mathbf{PT}_h\mathbf{y}$ w podprzestrzeni R^{M_h} poszukiwaną odległość oblicza się ze wzoru:

$$\mathrm{d}_h(\mathbf{x},\mathbf{y}) = d_h(\boldsymbol{x}_h,\boldsymbol{y}_h) = \sqrt{(\boldsymbol{x}_h - \boldsymbol{y}_h)^T \mathbf{Q}_h^{-1}(\boldsymbol{x}_h - \boldsymbol{y}_h)}, \quad \mathbf{x},\mathbf{y} \in R^L \tag{20}$$

Metryka ta może być wykorzystywana do wyznaczania odległości między obserwacją $\mathbf{x}$ a klastrem $C(W_h)$. Przykładowo, odległość między obserwacją $\mathbf{x}$ a klastrem $C(W_h)$ dla metody centroidalnej jest określona wzorem:

$$\mathrm{D}_h^{(1)}(\mathbf{x}, C(W_h)) = d_h(\boldsymbol{x}_h, \overline{\boldsymbol{w}}_h) = \sqrt{(\boldsymbol{x}_h - \overline{\boldsymbol{w}}_h)^T \mathbf{Q}_h^{-1}(\boldsymbol{x}_h - \overline{\boldsymbol{w}}_h)} \tag{21}$$

gdzie: $\boldsymbol{x}_h = \mathbf{PT}_h\mathbf{x}$, $\overline{\boldsymbol{w}}_h = \mathbf{PT}_h\overline{\mathbf{w}}_h$, a wektor $\overline{\mathbf{w}}_h$ jest zdefiniowany przez (9).

6.2. Metoda obliczania odległości wektora obserwacji od podprzestrzeni wzorca

Metoda ta polega na bezpośrednim obliczaniu odległości między obserwacją $\mathbf{x}$ a klastrem $C(W_h)$. Odległość ta jest wyznaczana w przestrzeni cech R^L jako odległość między obserwacją $\mathbf{x}$ a jej rzutem $\mathbf{x}_h$ na podprzestrzeń wzorca $C(W_h)$:

$$\mathrm{D}_h^{(2)}(\mathbf{x}, C(W_h)) = \mathrm{d}(\mathbf{x}, \mathbf{x}_h) = \sqrt{(\mathbf{x}-\mathbf{x}_h)^T \mathbf{R}^{-1}(\mathbf{x}-\mathbf{x}_h)} \tag{22}$$

gdzie:

$$\mathbf{x}_h = \mathbf{T}_h^{-1} z + \overline{\mathbf{w}}_h \tag{23}$$

$$z = \mathbf{P}\mathbf{z} = \begin{bmatrix} z_1 \\ \cdots \\ z_{M_h} \\ 0 \\ \cdots \\ 0 \end{bmatrix}, \qquad \mathbf{z} = \begin{bmatrix} z_1 \\ \cdots \\ z_{M_h} \\ z_{M_h+1} \\ \cdots \\ z_L \end{bmatrix} = \mathbf{T}_h(\mathbf{x} - \overline{\mathbf{w}}_h) \tag{24}$$

6.3. Porównywanie odległości

Porównywanie odległości dopasowanych do różnych wzorców wymaga normalizacji. Jej celem jest spełnienie dla każdego wzorca następującego warunku: wartość oczekiwana znormalizowanej odległości $\overline{\mathrm{D}}_h^{(i)}(\mathbf{x}, C(W_h))$ ma wartość 1 [4]. Obliczenie wartości znormalizowanej określa następujący wzór:

$$\overline{\mathrm{D}}_h^{(i)}(\mathbf{x}, C(W_h)) = \frac{1}{\sqrt{N_h}} \mathrm{D}_h^{(i)}(\mathbf{x}, C(W_h)), \quad i = 1,2 \tag{25}$$

6.4. Skalaryzacja wektora odległości

Wykorzystywanie obydwu metod oceny odległości analizowanego punktu $\mathbf{x}$ przestrzeni obserwacji R^L od wzorca W_h daje możliwość wektorowej oceny tej odległości; jej wynikiem są odległości $\overline{\mathrm{D}}_h^{(1)}(\mathbf{x}, C(W_h))$ oraz $\overline{\mathrm{D}}_h^{(2)}(\mathbf{x}, C(W_h))$.

Ocena druga przyjmuje wartość zerową wtedy, gdy podprzestrzeń wzorca nie jest właściwa, tzn. gdy $R^{M_h} = R^L$. Łatwo stwierdzamy, że jeśli $M_h = L$, to $\boldsymbol{z} = \mathbf{z}$. W konsekwencji $\mathbf{x} - \mathbf{x}_h = \mathbf{x} - \mathbf{T}_h^{-1}\boldsymbol{z} - \overline{\mathbf{w}}_h = \mathbf{x} - \mathbf{T}_h^{-1}\mathbf{T}_h(\mathbf{x} - \overline{\mathbf{w}}_h) - \overline{\mathbf{w}}_h = \mathbf{0}$. Zatem wtedy $\mathrm{D}_h^{(2)}(\mathbf{x}, C(W_h)) = 0$ dla wszystkich $\mathbf{x} \in R^L$.

Liniowe uporządkowanie według wektorowych obliczeń odległości można uzyskać, stosując dowolną metodę skalaryzacji wektora odległości. Przykładowo, zastosowanie wzoru:

$$\overline{\mathrm{D}}_h^{\mathrm{s}}(\mathbf{x}, C(W_h)) = \sqrt{\left[\overline{\mathrm{D}}_h^{(1)}(\mathbf{x}, C(W_h))\right]^2 + \left[\overline{\mathrm{D}}_h^{(2)}(\mathbf{x}, C(W_h))\right]^2} \tag{26}$$

umożliwia „gładkie" przejście od oceny z dominacją wartości $\overline{\mathrm{D}}_h^{(2)}(\mathbf{x}, C(W_h))$ do oceny wyłącznie na podstawie wartości $\overline{\mathrm{D}}_h^{(1)}(\mathbf{x}, C(W_h))$. Sytuacja taka może mieć miejsce w przypadku wzbogacania wzorca W_h przez wskazywanie nowych jego przykładów.

7. Eksperyment

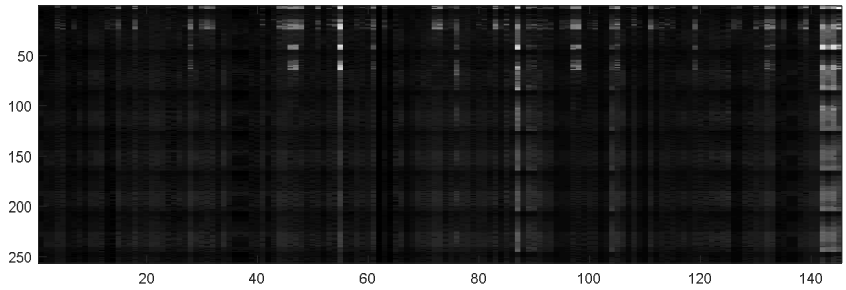
7.1. Przedmiot i cel badań

W celu zilustrowania proponowanych metod dokonano analizy przykładowego zbioru wyników pomiaru[1]. Pojedynczy wynik pomiaru stanowi wektor, którego współrzędne były wyznaczone jako wyniki benchmarków. Każdy pomiar wykonywany był na innym zestawie komputerowym, współrzędne o jednakowym indeksie opisują wynik tego samego benchmarku. Zestawy miały różną konfigurację sprzętową i programową, tzn. różniły się albo procesorami, albo płytami głównymi, albo systemami operacyjnymi, albo zainstalowanym, aktywnym oprogramowaniem i otoczeniem sieciowym. Wykorzystywany zbiór danych zawierał wyniki 256 benchmarków wyznaczone dla 145 zestawów. Wizualizację tych wyników pomiaru w postaci obrazu przedstawiono na rysunku 3.

Istotną cechą zastosowanej metody analizy jest brak wymagania znajomości charakterystyk analizowanego zbioru danych – zadanego po prostu w postaci macierzy. Jako wzorzec zachowania normalnego wskazano 19 zestawów bazujących na procesorze typu A. Jako wzorzec alternatywny zostało

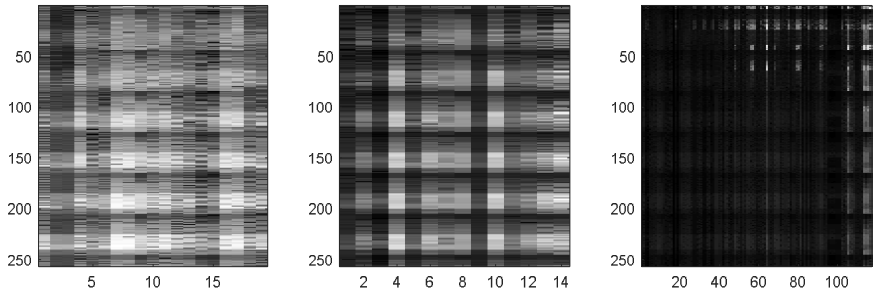
[1] Do obliczeń zostały wykorzystane wyniki pomiarów udostępnione mi przez ich autora, Artura Miktusa (artur.miktus@wat.edu.pl).

wskazanych 14 zestawów bazujących na procesorach typu B. Przy tak wybranych wzorcach analiza polegała na określeniu, które z badanych zestawów zachowują się jak zestawy wzorcowe wyposażone w procesory typu A, a które jak zestawy wzorcowe wyposażone w procesory typu B.



Rys. 3. Wizualizacja źródłowych wyników pomiaru w postaci obrazu. Wyniki pomiaru są liczbami dodatnimi. Stopień szarości odpowiada wartości liczbowej elementu macierzy. Liczba wierszy jest równa liczbie współrzędnych wektora pomiaru 256, liczba kolumn jest równa liczbie zestawów 145.

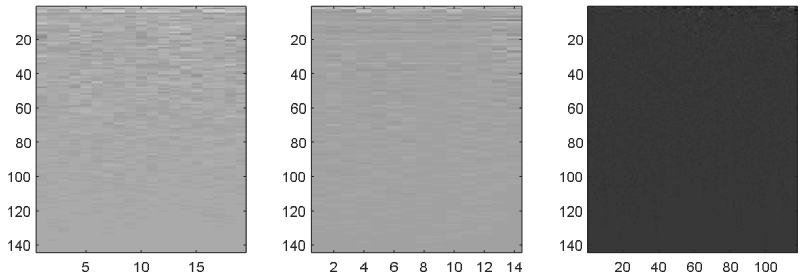
Do testowania wybrano arbitralnie 117 zestawów, dla których wskazany przykładami rodzaj anomalii nie był oczekiwany. W zbiorze wybranych do testowania zestawów umieszczono też zestawy wskazane jako wzorce zachowania normalnego. Wizualizacja macierzy pomiarów dla wskazanych zestawów wzorcowych oraz zestawów testowanych została przedstawiona na rysunku 4.



Rys. 4. Wizualizacja macierzy pomiarów: na rysunku z lewej dla wzorca W_1, na rysunku w środku dla wzorca W_2 oraz na rysunku z prawej dla zestawów testowanych. Liczba przykładów wzorca W_1 jest równa $N_1 = 19$, liczba przykładów wzorca W_2 jest równa $N_2 = 14$, liczba zestawów testowanych $N_a = 117$.

7.2. Przetwarzanie wstępne

Celem wstępnego przetwarzania analizowanych danych była redukcja liczby pomiarów, tak aby odpowiadająca im macierz kowariancji była dodatnio określona. Rezultat ten został osiągnięty poprzez wyznaczenie składowych głównych o niezerowej wariancji. Liczba takich składowych wyniosła 144. Uzyskana macierz składowych głównych była podstawą dalszej analizy i nazywana jest dalej macierzą wyników obserwacji. Odpowiednie wartości parametrów w przedstawianym przykładzie są więc następujące: liczba wszystkich przykładów zachowań $N = 145$, liczba wskazanych przykładów dla wzorca pierwszego $N_1 = 19$, liczba wskazanych przykładów dla wzorca drugiego $N_2 = 14$, liczba współrzędnych wektora obserwacji $L = 144$. Przedmiotem analizy jest więc 145 wektorów obserwacji, a każdy wektor obserwacji ma 144 współrzędnych. $L = 144$. Wizualizację obliczonych wyników obserwacji dla wskazanych przykładów wzorców oraz testowanych zestawów przedstawiono na rysunku 5.

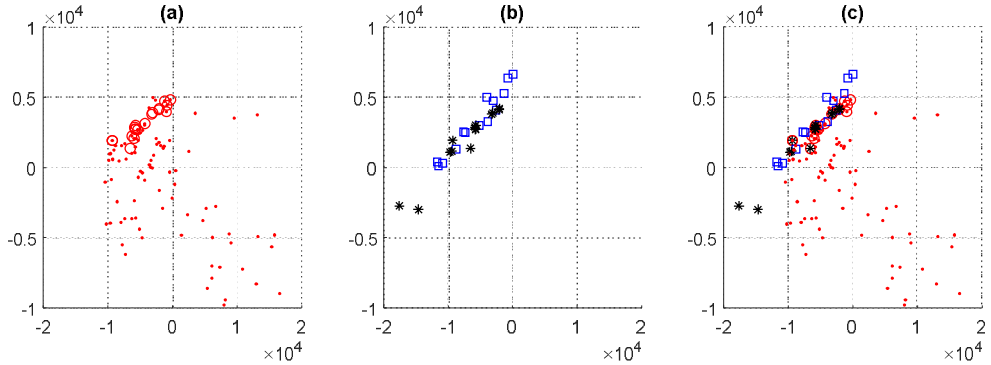


Rys. 5. Wizualizacja macierzy obserwacji: na rysunku z lewej dla wzorca W_1, na rysunku w środku dla przykładów wzorca W_2 oraz na rysunku z prawej dla testowanych zestawów. Liczba współrzędnych wektora składowych głównych jest równa $L = 144$, liczba przykładów wzorca W_1 jest równa $N_1 = 19$, liczba przykładów wzorca W_2 jest równa $N_2 = 14$, liczba testowanych zestawów jest równa $N_a = 117$.

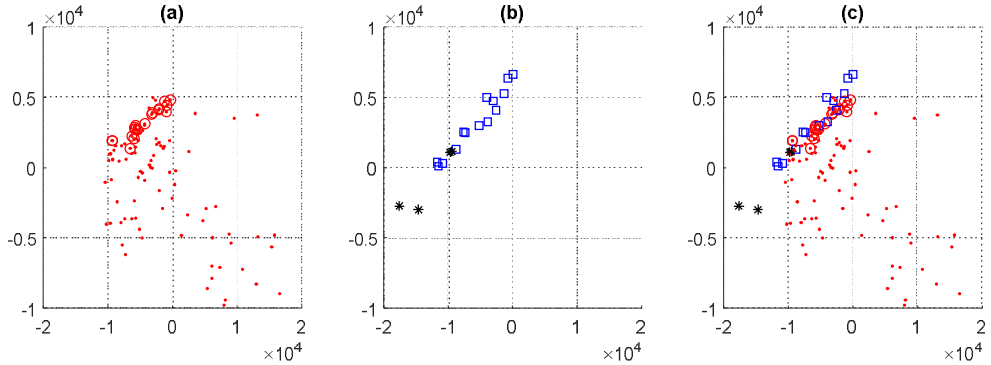
7.3. Wyniki analizy

W przedstawianym przykładzie podprzestrzeń wzorca W_1 ma wymiar $M_1 = 18$, a podprzestrzeń wzorca W_2 ma wymiar $M_2 = 13$. Porównanie odległości badanego wektora obserwacji $\mathbf{x} \in R^{144}$ od klastra $C(W_1)$ wzorca W_1 i odległości badanego wektora obserwacji $\mathbf{x} \in R^{144}$ od klastra $C(W_2)$ wzorca

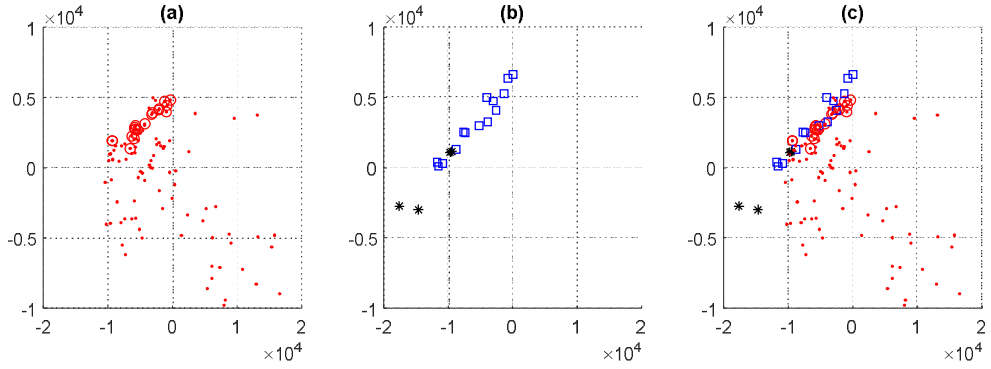
W_2 zostało wykonane dla odległości $\overline{\mathrm{D}}_h^{(1)}(\mathbf{x}, C(W_h))$, $\overline{\mathrm{D}}_h^{(2)}(\mathbf{x}, C(W_h))$ oraz $\overline{\mathrm{D}}_h^{\mathrm{s}}(\mathbf{x}, C(W_h))$. Wyniki porównań zostały zobrazowane na rysunkach 6-11.



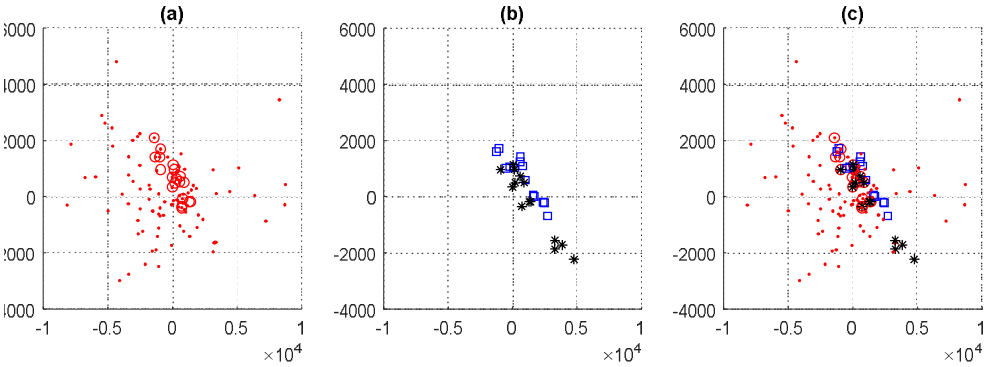
Rys. 6. Wizualizacja wyników analizy w podprzestrzeni pierwszych dwóch współrzędnych wektorów obserwacji na podstawie porównania odległości $\overline{\mathrm{D}}_h^{(1)}(\mathbf{x}, C(W_h))$. (a) Wzorce normalności W_1 są oznaczone kółkami, punktami oznaczono wyniki obserwacji ocenione jako normalne. (b) Wzorce anomalii W_2 są oznaczone kwadratami, gwiazdkami oznaczono wyniki obserwacji ocenione jako anomalne. (c) Nałożenie wykresów (a) oraz (b).



Rys. 7. Wizualizacja wyników analizy w podprzestrzeni pierwszych dwóch współrzędnych wektorów obserwacji na podstawie porównania odległości $\overline{\mathrm{D}}_h^{(2)}(\mathbf{x}, C(W_h))$. (a) Wzorce normalności W_1 są oznaczone kółkami, punktami oznaczono wyniki obserwacji ocenione jako normalne. (b) Wzorce anomalii W_2 są oznaczone kwadratami, gwiazdkami oznaczono wyniki obserwacji ocenione jako anomalne. (c) Nałożenie wykresów (a) oraz (b).



Rys. 8. Wizualizacja wyników analizy w podprzestrzeni pierwszych dwóch współrzędnych wektorów obserwacji na podstawie porównania odległości $\overline{\mathrm{D}}_h^{\mathrm{s}}(\mathbf{x}, C(W_h))$. (a) Wzorce normalności W_1 są oznaczone kółkami, punktami oznaczono wyniki obserwacji ocenione jako normalne. (b) Wzorce anomalii W_2 są oznaczone kwadratami, gwiazdkami oznaczono wyniki obserwacji ocenione jako anomalne. (c) Nałożenie wykresów (a) oraz (b).

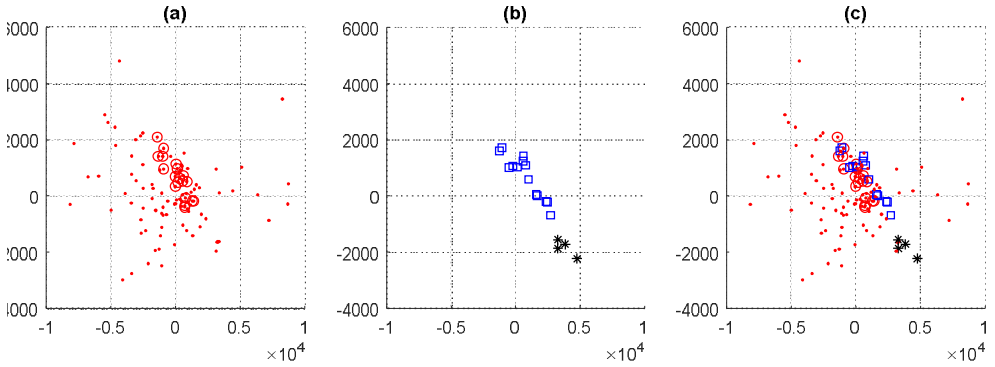


Rys. 9. Wizualizacja wyników analizy w podprzestrzeni współrzędnych o indeksach 3 i 4 wektorów obserwacji na podstawie porównania odległości $\overline{\mathrm{D}}_h^{(1)}(\mathbf{x}, C(W_h))$. (a) Wzorce normalności W_1 są oznaczone kółkami, punktami oznaczono wyniki obserwacji ocenione jako normalne. (b) Wzorce anomalii W_2 są oznaczone kwadratami, gwiazdkami oznaczono wyniki obserwacji ocenione jako anomalne. (c) Nałożenie wykresów (a) oraz (b).

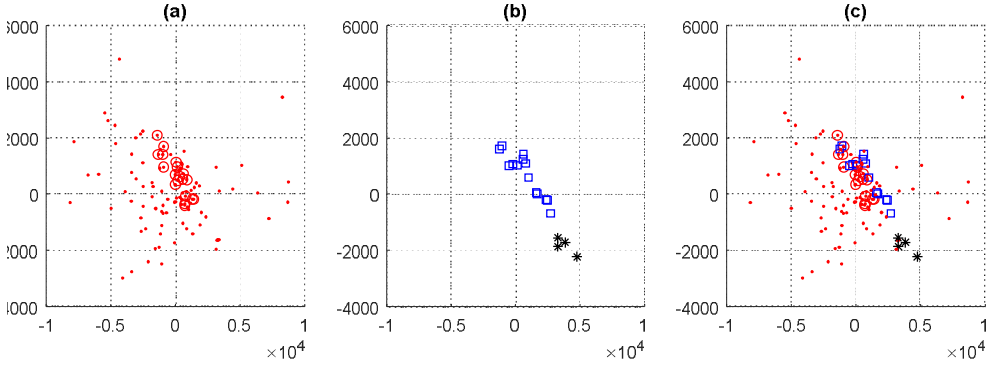
Ostateczny wynik obliczeń stanowi wskazanie, które z badanych zestawów były bliższe wzorcowi normalności, a które – wzorcowi alternatywnemu, interpretowanemu jako wzorzec anomalii. Na podstawie analizy odległości w podprzestrzeniach wzorców wykryto 14 przypadków anomalii (por. rys. 6 i rys. 9). Na podstawie analizy odległości obserwacji od podprzestrzeni wzorca

wykryto 4 przypadki (rys. 7, rys. 10), które pokrywają się z wykryciami na podstawie odległości sumarycznej (rys. 8, rys. 11).

Uzyskane wskazania anomalii mogą stanowić podstawę dodatkowej, szczegółowej analizy, mającej na celu przedstawienie przyczyn anomalii. W przeprowadzonym eksperymencie taka dodatkowa analiza była możliwa, ponieważ wszystkie zestawy i pomiary były dokładnie opisane.



Rys. 10. Wizualizacja wyników analizy w podprzestrzeni współrzędnych o indeksach 3 i 4 wektorów obserwacji na podstawie porównania odległości $\overline{\mathrm{D}}_h^{(2)}(\mathbf{x}, C(W_h))$. (a) Wzorce normalności W_1 są oznaczone kółkami, punktami oznaczono wyniki obserwacji ocenione jako normalne. (b) Wzorce anomalii W_2 są oznaczone kwadratami, gwiazdkami oznaczono wyniki obserwacji ocenione jako anomalne. (c) Nałożenie wykresów (a) oraz (b).



Rys. 11. Wizualizacja wyników analizy w podprzestrzeni współrzędnych o indeksach 3 i 4 wektorów obserwacji na podstawie porównania odległości $\overline{\mathrm{D}}_h^{\mathrm{s}}(\mathbf{x}, C(W_h))$. (a) Wzorce normalności W_1 są oznaczone kółkami, punktami oznaczono wyniki obserwacji ocenione jako normalne. (b) Wzorce anomalii W_2 są oznaczone kwadratami, gwiazdkami oznaczono wyniki obserwacji ocenione jako anomalne. (c) Nałożenie wykresów (a) oraz (b).

Szczegółowa analiza opisu zestawów i warunków pomiarów (ustalająca przyczyny uzyskania obserwacji odbiegających od wzorcowych) może być podstawą orzeczenia o wystąpieniu ewentualnego błędu detekcji: fałszywego alarmu lub fałszywego spokoju, a także przedstawienia wniosków o zasadach optymalizacji dwukryterialnej (np. przez określenie ważonej odległości sumarycznej).

8. Wnioski końcowe

1) Proponowane metody detekcji anomalii mają charakter uniwersalny i mogą być wykorzystywane wszędzie tam, gdzie wyniki zachowania systemu można traktować jako pomiary zapisywane w postaci wektorów liczb rzeczywistych. Nie jest potrzebne opracowanie żadnych modeli powstawania wykorzystywanych wyników pomiarów.

2) Definiowanie normalności sprowadza się do wskazania odpowiednich przykładów. Wskazanie przykładów anomalii pozwala uprościć wnioskowanie dzięki możliwości porównywania dwóch odległości obserwowanego zachowania systemu: od wskazanych przykładów zachowania normalnego i analogicznej odległości od wskazanych przykładów zachowania anomalnego. Wynikiem wnioskowania jest wskazanie systemów, dla których wyniki obserwacji ich zachowań odbiegają od wskazanych przykładów zachowań wzorcowych.

3) Przedstawione dwie zasadnicze metody obliczania odległości mogą być wykorzystywane dowolnie, w zależności od badanego systemu. Zastosowanie łączne prowadzi do optymalizacji wektorowej. W przypadku wskazania wystarczająco dużo przykładów wzorca (w stosunku do wymiaru wektora obserwacji) odległość analizowanej obserwacji od podprzestrzeni wzorca staje się zerowa i w ten sposób uzyskuje się płynne przejście do oceny odległości tylko na podstawie metryki w przestrzeni wzorca.

4) Przedstawione metody obliczeniowe pozwalają na analizę w sytuacji, gdy wymiar wektora pomiaru jest większy od liczby wskazanych przykładów wzorca. Z reguły dotyczy to wzorców anomalii. Sytuacja taka występuje praktycznie wtedy, gdy wyniki obserwacji systemu nie są selekcjonowane pod kątem ich użyteczności w zadaniach detekcji anomalii. Dotyczy to zwłaszcza zadań wykrywania anomalii na podstawie danych generowanych automatycznie, zwykle przeznaczonych do innych celów.

5) Tworzenie wzorców przez wskazywanie przykładów można traktować jako sposób łączenia (syntezy, fuzji) informacji pochodzących z różnych źródeł.

Łączenie to ma charakter sekwencyjny w tym sensie, że wskazywane przykłady są uzyskiwane na podstawie obserwacji z innych źródeł.

Literatura

[1] CAMPOS G.O, ZIMEK A., SANDER J., CAMPELLO R.J.G.B., MICENKOVÁ B., SCHUBERT E., ASSENT I., HOULE M.E., *On the evaluation of unsupervised outlier detection: measures, datasets, and an empirical study.* Data Mining and Knowledge Discovery 30(4), 2016, pp. 891-927.

[2] CHANDOLA V., BANERJEE A., KUMAR V., *Anomaly detection: A survey*. ACM Computing Surveys, Vol. 41, No. 3, Article 15, 2009.

[3] HODGE V.J.; AUSTIN J., *A survey of outlier detection methodologies*. Artificial Intelligence Review, 22 (2), 2004, pp. 85-126.

[4] KWIATKOWSKI W., *Metody automatycznego rozpoznawania wzorców*, BEL, Warszawa, 2010.

[5] SODEMANN A.A., ROSS M.P., BORGHETTI B.I., *A review of anomaly detection in automated surveillance*. IEEE Transactions on Systems Man and Cybernetics Part C (Applications and Reviews), Vol. 42 no. 6, 2012 pp. 1257-1272.

[6] PIMENTEL M.A., CLIFTON D.A., CLIFTON L., TARASSENKO L., *A review of novelty detection*. Signal Processing, Vol. 99, 2014, pp. 215-249.

[7] TUKEY J.W., *Exploratory data analysis*. Addison-Wesley, 1977.

[8] YAO-GUANG WEI, DE-LING ZHENG, YING WANG, *Research of a negative selection algorithm and its application in anomaly detection*. Proceedings of 2004 International Conference on Machine Learning and Cybernetics (IEEE Cat. No.04EX826), Vol. 5, 2004, pp. 2910-2913.

[9] ZIMEK A., SCHUBERT E., KRIEGEL H., *A survey on unsupervised outlier detection in high-dimensional numerical data*. Statistical Analysis and Data Mining, Vol. 5, Issue 5, 2012, pp. 363-387.

Anomaly detection based on given examples

ABSTRACT: The paper considers the issue of anomalies detection based on registered observations of a system behavior. The problem is formulated as recognition of normal and anomalous behavior patterns. Both types of patterns are identified by indication of appropriate examples. A peculiarity of this task is that usually the number of examples is far lower than the dimension of vectors describing the observations. Two methods to solve this task have been presented in the paper, based on projecting the observations on the subspace of examples. The first method is based on a distance of the observation vector from the subspace of examples. The second method is based on transferring the pattern recognition problem to the subspace of examples.

KEYWORDS: anomaly detection, novelty detection, outlier detection, pattern recognition, exploratory data analysis, Mahalanobis distance

Praca wpłynęła do redakcji: 18.05.2018 r.