Macierzowy cyfrowy cień sieci czujników IoT

Władysław Iwaniec
Akademia Tarnowska w Tarnowie, Wydział Politechniczny, Katedra Automatyki i Robotyki, ul. Mickiewicza 8, 33-100 Tarnów

Streszczenie: W artykule przedstawiono koncepcję macierzowego cyfrowego cienia sieci czujników IoT. Omówiono różnice między cyfrowym bliźniakiem a cyfrowym cieniem i uzasadniono wybór koncepcji cienia sieci czujników. Przedstawiono macierzowy opis takiej sieci i wprowadzono koncepcję ε_k – sąsiedztwa czujnika. Zamieszczono wzory dla modeli liniowych ε_k – sąsiedztw typu plus i typu gwiazdka. Na wybranych przykładach pokazano możliwość wykrywania i eliminacji niektórych zagrożeń bezpieczeństwa takiej sieci.

Słowa kluczowe: cienie cyfrowe, bezpieczeństwo, Internet Rzeczy, zagrożenia bezpieczeństwa, urządzenia IoT, sieci czujników, modele macierzowe

1. Wprowadzenie

Sieci czujników, zwłaszcza bezprzewodowych WSN (ang. *Wireless Sensor Network*), są stosowane w wielu obszarach, w tym w rolnictwie, inteligentnych budynkach, medycynie czy monitorowaniu środowiska. Zestawy czujników, które mierzą wartość tej samej wielkości fizycznej lub chemicznej, np. temperatury, ciśnienia, wilgotności, zakwaszenia gleby są narażone na ataki lub awarie, w szczególności wskutek zużycia energii, podstawienia fałszywego czujnika czy przejęcia nad nim lub jego kanałem komunikacyjnym kontroli przez intruza.

Sieci WSN dla czujników są podatne na rozmaite ataki, zwłaszcza w obszarze transmisji danych [1]. Przeprowadzona analiza i przegląd literatury [2] wskazują na znaczenie incydentu polegającego na przejęciu jednego z węzłów, który naśladuje pracę rzetelnego (prawowitego) węzła i zakłóca pracę układu. Pokazano, że istnieją różne metody, zgodne z zasadą CIA, ochrony sieci WSN przed naruszeniem bezpieczeństwa, w szczególności związane z ochroną kryptograficzną, jednakże nie dają one możliwości oceny danych generowanych przez czujniki. W przeglądowym artykule [3] zamieszczono m.in. analizę metod maszynowego uczenia się stosowanych do poprawy bezpieczeństwa bezprzewodowych sieci czujników, w szczególności opartą na algorytmie k-nn. Wykorzystanie idei najbliższych sąsiadów do budowy cyfrowego cienia DS (ang. *Digital Shadow*) siatki czujników pozwala na podniesienie poziomu jej bezpieczeństwa, w szczególności przez eliminację, względnie minimalizację wpływu fałszywych lub zakłóconych danych na zachowanie układu, a zwłaszcza na sterowanie. W kolejnym przeglądowym artykule [4] przedstawiającym rozmaite zagadnienia bezpieczeństwa Internetu Rzeczy przedyskutowane zostały m.in. różne architektury IoT. Jedno z podejść, wybrane przez autorów ze względu na „intuicyjny charakter architektury", wyróżnia trzy warstwy: warstwę wykrywania lub percepcji, warstwę sieciową i warstwę aplikacji. Przedstawiony cień cyfrowy sieci czujników jest usytuowany w warstwie aplikacji, ale jego zadaniem jest poprawa bezpieczeństwa tej sieci przez wykrywanie i eliminację anomalii i błędów zarówno w warstwie percepcji, jak też w warstwie sieciowej.

Autor korespondujący:
Władysław Iwaniec, wiw@atar.edu.pl

Artykuł recenzowany
nadesłany 13.12.2024 r., przyjęty do druku 05.02.2025 r.

2. Cyfrowe bliźniaki i cyfrowe cienie

David Gelernter przedstawił ideę cyfrowego bliźniaka [5], wskazując na możliwości odwzorowania świata rzeczywistego za pomocą metod symulacyjnych. Formalnie pierwszy raz ten termin został użyty w raporcie NASA z 2010 r., chociaż już w 2002 r. Michael Grieves przedstawił jego koncepcję na konferencji związanej z inteligentnymi systemami wytwórczymi w branży lotniczej. Agencja NASA zaproponowała w 2012 r. następującą definicję [6, 7]: "Bliźniak cyfrowy to zintegrowana, wielofizyczna, wieloskalowa, probabilistyczna symulacja złożonego produktu, która stosuje najlepszy z dostępnych modeli fizycznych, dane z sensorów w czasie rzeczywistym, dane historyczne itp., aby odzwierciedlić funkcjonowanie odpowiadającego mu bliźniaka". W oryginalnej koncepcji bliźniaka cyfrowego M. Grieves zwrócił uwagę na fundamentalne znaczenie wzajemnego przepływu informacji między bliźniakami i oddziaływania cyfrowej repliki na układ fizyczny w czasie rzeczywistym.

W późniejszych przeglądowych pracach [8, 9] autorzy przedstawili rozmaite podejścia do tej definicji i możliwość wyróżnienia wśród analizowanych rozmaitych odmian cyfrowych odwzorowań tzw. cyfrowego cienia. Różnice między cyfrowym cieniem a cyfrowym bliźniakiem zostały przedstawione m.in. w [10]. W opracowaniu [21] przyjęto, że „cyfrowy cień" jako pole działania w Przemyśle 4.0 to „wystarczająco dokładny" obraz procesów „w obszarach produkcji, rozwoju i pokrewnych, w celu stworzenia podstawy oceny wszystkich istotnych danych w czasie rzeczywistym". W celu utworzenia takiego cienia należy najpierw określić i utworzyć bazę danych z różnych źródeł danych, na przykład z produkcji lub rozwoju, następnie je przefiltrować, dokonać ich agregacji i dopiero wtedy poddać dalszemu przetwarzaniu. Takie podejście, w którym na podstawie zmierzonych wartości tworzy się model układu, pozwalający na „ocenę

wszystkich istotnych danych w czasie rzeczywistym" może być zastosowane również do zestawu urządzeń IoT, które są źródłem danych pomiarowych.

W przywołanym artykule [8] podkreślono, że w publikacjach spotyka się określenia „cyfrowy model", „cyfrowy cień" i „cyfrowy bliźniak" dla rozróżnienia stopnia odwzorowania i wzajemnego oddziaływania świata rzeczywistego i wirtualnego. Taki podział spotkał się z krytyką [11], gdzie zwrócono uwagę na niedostatki zaproponowanego nazewnictwa i wskazano na potrzebę jednoznacznego posługiwania się pojęciem cyfrowego bliźniaka.

Mimo krytycznego stanowiska dotyczącego stosowanego nazewnictwa, dla analizowanego dalej rozwiązania, które jedynie odwzorowuje stan rzeczywisty, a następnie służy do przetwarzania uzyskanych danych w celu oceny ich wiarygodności, nie oddziałując bezpośrednio na siatkę czujników, zastosowanie określenia „cyfrowego cienia" jest zdecydowanie bardziej trafne, niż pojęcia „cyfrowego bliźniaka".

Warto zauważyć, że trwają i postępują prace mające na celu ustalenie standardów dla cyfrowych replik świata rzeczywistego, w szczególności takie jak projekt NIST „Digital Twins for Advanced Manufacturing" [22] i norma ISO 23247, definiująca ramy wspierające tworzenie cyfrowych bliźniaków jako obserwowalnych elementów produkcyjnych, w tym personelu, sprzętu, materiałów, procesów produkcyjnych, obiektów, środowiska, produktów i dokumentów pomocniczych [12, 23].

3. Macierzowy cyfrowy cień wybranej klasy zestawu czujników

Zestawy czujników, obecnie najczęściej bezprzewodowych, ze względu na łatwość implementacji i względnie niskie koszty są stosowane do pomiarów rozmaitych wielkości fizykochemicznych w wielu układach automatyki. Takie zestawy są zazwyczaj połączone za pośrednictwem sieci z punktem odbioru pomiarów, a otrzymany strumień danych pomiarowych jest przetwarzany w celu uzyskania odpowiednich nastaw aktuatorów. Typowymi problemami bezpieczeństwa takich układów są ataki na pojedyncze sensory (węzły) sieci, awarie, utrata łączności z czujnikiem czy ograniczenia urządzenia związane ze zbyt małą pamięcią czy mocą obliczeniową [13]. Wskutek takich zagrożeń celowa jest ocena, czy wyniki pomiarów uzyskane i przesyłane przez każdy z czujników są rzetelne czy też fałszywe i czy należy je wtedy zastąpić danymi historycznymi z ostatniego poprawnego odczytu lub wartościami obliczonymi przez cień.

W pracy [14] przedstawiono koncepcję rozszerzenie modelu ochrony urządzeń IoT na brzegu sieci o macierze oddziaływań i powiązań. Zgodnie z zaproponowanym rozwiązaniem zakłada się, że ochronie podlega zbiór czujników tej samej wielkości fizykochemicznej, który przesyła dane do układu sterowania wyznaczającego sygnały dla urządzeń wykonawczych. Zakłada się, że czujniki mogą przesyłać dane niezależnie do urządzenia brzegowego BS (ang. *Border Station*), lecz nie mogą komunikować się bezpośrednio ze sobą. Do realizacji koncepcji ochrony takiego układu czujników przed atakami, polegającymi na podstawieniu czujnika czy falsyfikacji danych, może być zastosowany cyfrowy cień takiego zestawu. Założenie o jednorodności sensorów oznacza, że proponowany cień nie może być stosowany dla kolekcji czujników różnych wielkości fizycznych i oczywiście dla pojedynczych sensorów. W takich przypadkach dobre rezultaty można uzyskać stosując fuzję danych (rozumianą jako „Wielopoziomowy proces dotyczący powiazania, korelacji, połączenia danych i informacji z pojedynczego i większej liczby czujników, mający na celu osiągniecie dokładniejszej estymacji, kompletnej i terminowej oceny sytuacji, zagrożeń i ich znaczenia" [15, 24]) scharakteryzowaną m.in. w [16] i wykorzystującą filtr Kalmana [17]. Szeroki przegląd zastosowań w robotyce zarówno klasycznego filtru, jak i jego modyfikacji jest przedstawiony w [18].

Trzeba zaznaczyć, że proponowany cyfrowy cień różni się istotnie od dobrze znanych zastosowań filtru Kalmana. Podstawowe różnice wynikają z faktu wyznaczania macierzy współczynników cienia na podstawie wielu poprzednich wyników pomiarów (a więc „głębszej" historii) oraz na porównaniu wartości pomiaru w chwili t z wartością obliczoną przez cień dla tej chwili (na podstawie pomiarów uzyskanych przez sąsiednie czujniki także w tej chwili), a celem takiego porównania jest wykrycie anomalii w pracy sensora, a nie filtracja szumów.

W celu utworzenia „cyfrowego cienia" takiego układu rozważmy zestaw czujników tej samej wielkości fizykochemicznej, który może być rozpatrywany w układzie topologicznie równoważnym z siatką (kratą) sensorów usytuowanych w m rzędach po n czujników w każdym rzędzie; wtedy zbiór wartości zmierzonych w pewnej chwili t przez zbiór tych czujników można opisać macierzą:

$$C^t_{m\times n} = \begin{bmatrix} c_{11} & c_{12} & c_{13} & \cdots & c_{1n} \\ c_{21} & c_{22} & c_{23} & \cdots & c_{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_{m1} & c_{m2} & c_{m3} & \cdots & c_{mn} \end{bmatrix}, \tag{1}$$

gdzie c_{ij} oznacza wartość zmierzoną przez czujnik i,j w pewnej chwili t.

Jak stwierdzono wcześniej, porównanie wartości przesłanych przez czujnik z wartościami obliczonymi przez cień pozwala na stwierdzenie nieprawidłowości. W takim przypadku układ sterowania (w trybie awaryjnym) w miejsce wartości błędnych przyjmie wartości obliczone przez cień i jednocześnie powiadomi operatora o konieczności podjęcia właściwych procedur naprawczych. Warto zauważyć, że ze względu na utrzymywanie w pamięci cienia historii (w praktyce kilku) poprzednich pomiarów, cień mógłby także wystawić jako wynik do obliczenia sygnału sterującego jeden z poprzednio zapamiętanych pomiarów, np. ostatni poprawny, jednakże dla zmieniających się wartości mierzonej wielkości, lepsze rezultaty zapewni wystawienie wartości obliczonej przez cień, gdyż ta wartość uwzględnia zachodzące zmiany.

W pracy przyjęto, że cieniem wartości mierzonej przez każdy z rozważanych czujników będzie wartość funkcji określonej dla argumentów, którymi są wartości zmierzone przez sąsiednie czujniki, przy czym rozważany jest model liniowy i dwa typy sąsiedztw – sąsiedztwo typu „plus" i sąsiedztwo typu „gwiazdka".

Przez „ε_k — sąsiedztwo typu plus" dla czujnika mierzącego wartość c_{ij} należy rozumieć układ czujników, które mierzą wartości c_{uv}, przy czym wartości indeksu u albo indeksu v różnią się od wartości indeksów i albo j co najwyżej o wartość k.

Przykład

Dla ε_1 — sąsiedztwa typu plus wartości c^*_{ij} dla cienia rzeczywistej wartości, c_{ij} wyznaczane są z zależności:

$$c^*_{ij} = \alpha_{i-1j}c_{i-1j} + \alpha_{ij-1}c_{ij-1} + \alpha_{i+1j}c_{i+1j} + \alpha_{ij+1}c_{ij+1}, \tag{2}$$

gdzie: $i \in \{1,2,\ldots,m\}$, $j \in \{1,2,\ldots,n\}$, przy czym dla indeksów niedodatnich lub odpowiednio większych od m albo n (dla czujników usytuowanych w narożach lub na brzegu siatki) wartości α_{uv} przyjmuje się równe 0.

Dla ε_2 — sąsiedztwa typu plus wartości c_{ij}^* dla cienia rzeczywistej wartości, c_{ij} wyznaczane są z zależności:

$$\begin{aligned} c_{ij}^* &= \alpha_{i-2j}c_{i-2j} + \alpha_{i-1j}c_{i-1j} + \alpha_{ij-2}c_{ij-2} + \alpha_{ij-1}c_{ij-1} \\ &+ \alpha_{i+1j}c_{i+1j} + \alpha_{i+2j}c_{i+2j} + \alpha_{ij+1}c_{ij+1} + \alpha_{ij+2}c_{ij+2} \end{aligned} \tag{3}$$

Ogólnie, dla ε_k — sąsiedztwa typu plus wartości c_{ij}^* cienia rzeczywistej wartości c_{ij} wyznaczane są z zależności (w postaci wektorowej):

$$\left[\alpha_{uv}\right] \cdot \left[c_{uv}\right]^{\mathrm{T}}, \tag{4}$$

gdzie:

$$\begin{aligned} \left[\alpha_{uv}\right] = [&\alpha_{i-kj}, \alpha_{i-(k-1)j}, \ldots, \alpha_{i-1j}, \alpha_{ij-k}, \alpha_{ij-(k-1)}, \ldots, \alpha_{ij-1}, \\ &\alpha_{i+1j}, \ldots, \alpha_{i+(k-1)j}, \alpha_{i+kj}, \alpha_{ij+1}, \ldots, \alpha_{ij+(k-1)}, \alpha_{ij+k}] \end{aligned}$$

$$\begin{aligned} \left[c_{uv}\right] = [&c_{i-kj}, c_{i-(k-1)j}, \ldots, c_{i-1j}, c_{ij-k}, c_{ij-(k-1)}, \ldots, c_{ij-1}, \\ &c_{i+1j}, \ldots, c_{i+(k-1)j}, c_{i+kj}, c_{ij+1}, \ldots, c_{ij+(k-1)}, c_{ij+k}] \end{aligned}$$

Przez „ε_k — sąsiedztwo typu gwiazdka" dla czujnika mierzącego wartość c_{ij} należy rozumieć układ czujników, które mierzą wartości c_{uv}, przy czym wartości indeksu u lub indeksu v nie różnią się od i lub j o więcej niż k.

Przykład

Dla ε_1 — sąsiedztwa typu gwiazdka wartości c_{ij}^* dla cienia rzeczywistej wartości, c_{ij} wyznaczane są z zależności:

$$\begin{aligned} c_{ij}^* &= \alpha_{i-1j}c_{i-1j} + \alpha_{ij-1}c_{ij-1} + \alpha_{i+1j}c_{i+1j} + \alpha_{ij+1}c_{ij+1} \\ &+ \beta_{i-1j-1}c_{i-1j-1} + \beta_{i-1j+1}c_{i-1j+1} + \beta_{i+1j+1}c_{i+1j+1} + \beta_{i+1j-1}c_{i+1j-1}, \end{aligned} \tag{5}$$

gdzie: $i \in \{1,2,\ldots,m\}$, $j \in \{1,2,\ldots,n\}$, przy czym dla indeksów niedodatnich lub odpowiednio większych od m albo n (dla czujników usytuowanych w narożach lub na brzegu siatki) wartości α_{uv} i β_{uv} przyjmuje się równe 0.

Ogólnie, dla ε_k — sąsiedztwa typu gwiazdka wartości c_{ij}^* cienia rzeczywistej wartości c_{ij} wyznaczane są z zależności (w postaci wektorowej):

$$\left[\alpha_{uv}\right] \cdot \left[c_{uv}\right]^{\mathrm{T}} + \left[\beta_{wz}\right] \cdot \left[c_{wz}\right]^{\mathrm{T}}, \tag{6}$$

gdzie:

$$\begin{aligned} \left[\alpha_{uv}\right] = [&\alpha_{i-kj}, \alpha_{i-(k-1)j}, \ldots, \alpha_{i-1j}, \alpha_{ij-k}, \alpha_{ij-(k-1)}, \ldots, \alpha_{ij-1}, \\ &\alpha_{i+1j}, \ldots, \alpha_{i+(k-1)j}, \alpha_{i+kj}, \alpha_{ij+1}, \ldots, \alpha_{ij+(k-1)}, \alpha_{ij+k}] \end{aligned}$$

$$\begin{aligned} \left[c_{uv}\right] = [&c_{i-kj}, c_{i-(k-1)j}, \ldots, c_{i-1j}, c_{ij-k}, c_{ij-(k-1)}, \ldots, c_{ij-1}, \\ &c_{i+1j}, \ldots, c_{i+(k-1)j}, c_{i+kj}, c_{ij+1}, \ldots, c_{ij+(k-1)}, c_{ij+k}] \end{aligned}$$

$$\begin{aligned} \left[\beta_{wz}\right] = [&\beta_{(i-k)(j-k)}, \beta_{(i-k+1)(j-k+1)}, \ldots, \beta_{(i-1)(j-1)}, \beta_{(i-k)(j+k)}, \beta_{(i-k+1)(j-k+1)}, \ldots, \beta_{(i-1)(j+1)}, \\ &\beta_{(i+k)(j+k)}, \ldots, \beta_{(i+1)(j+1)}, \beta_{(i+1)(j-1)}, \ldots, \beta_{(i+k-1)(j-k+1)}, \beta_{(i+k)(j-k)}] \end{aligned}$$

$$\begin{aligned} \left[c_{wz}\right] = [&c_{(i-k)(j-k)}, c_{(i-k+1)(j-k+1)}, \ldots, c_{(i-1)(j-1)}, c_{(i-k)(j+k)}, c_{(i-k+1)(j-k+1)}, \ldots, c_{(i-1)(j+1)}, \\ &c_{(i+k)(j+k)}, \ldots, c_{(i+1)(j+1)}, c_{(i+1)(j-1)}, \ldots, c_{(i+k-1)(j-k+1)}, c_{(i+k)(j-k)}]. \end{aligned}$$

Problem analitycznych podstaw wyboru typu sąsiedztwa i wartości k wymaga dalszych badań, mających na celu w szczególności klasyfikację cieni w zależności od środowiska, mierzonej wielkości i usytuowania czujników.

4. Wyznaczanie wartości współczynników macierzowego liniowego cienia zestawu czujników

W celu wyznaczenia wartości współczynników $[\alpha_{uv}]$ lub $[\alpha_{uv}]$ i $[\beta_{wz}]$ każdego elementu cienia, konieczne jest rozwiązanie odpowiedniego układu równań liniowych:

- dla ε_k — sąsiedztwa typu plus: układu $4k$ równań,
- dla ε_k — sąsiedztwa typu gwiazdka: układu $8k$ równań, uzyskiwanych w wyniku podstawienia w równaniach (4) lub (6) za c_{ij}^* wartości c_{ij} zmierzonych w kolejnych chwilach 1, 2, ..., p i zapisywanych w macierzy trójwymiarowej $\mathbf{B}_{m\times n\times p}$, gdzie, odpowiednio, $p \geqslant 4k$ lub $p \geqslant 8k$.

Dla cieni czujników ε_k — sąsiedztwa typu plus, które są usytuowane w narożach siatki czujników, układ równań (4) upraszcza się do układu $2k$ równań, a sąsiedztwo można nazwać sąsiedztwem typu gamma, a dla cieni czujników, które są na brzegu siatki, układ równań (4) upraszcza się do układu $3k$ równań, a sąsiedztwo można nazwać sąsiedztwem typu T.

Analogicznie, dla cieni czujników ε_k — sąsiedztwa typu gwiazdka, które są usytuowane w narożach siatki czujników, układ równań (6) upraszcza się do układu $3k$ równań, a sąsiedztwo można nazwać sąsiedztwem typu kwadrat, a dla cieni czujników, które są na brzegu siatki układ, równań (6) upraszcza się do układu $5k$ równań, a sąsiedztwa można nazwać sąsiedztwem typu prostokąt.

Na podstawie wyznaczonych wartości wektorów $[\alpha_{uv}]$ w kolejnych chwilach możliwe jest obliczenie wartości cienia, porównanie jej z wartością zmierzoną, obliczenie błędu względnego

$$\mathrm{delta}e_{ij} = \left(c_{ij}^* - c_{ij}\right) / c_{ij} \tag{7}$$

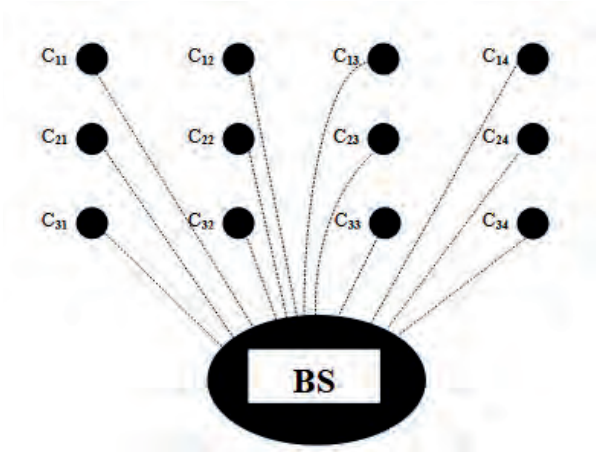
i wypracowanie rekomendacji o konieczności odrzucenia wartości zmierzonej jako wartości błędnej względnie ostrzeżenia, że zmierzona wartość może być błędna, w zależności od dopuszczalnej wartości błędu przyjętej polityki bezpieczeństwa. Dla arbitralnego określenia dopuszczalnych wartości błędu istotne znaczenie ma dokładność czujników.

Jak pokazano dalej na wybranych przykładach, zaprezentowany cyfrowy cień zestawu czujników pozwala na wykrycie i eliminację skutków utraty danych z czujnika, sfałszowania wartości przesyłanych danych oraz ataku podstawienia czujnika.

5. Przykład eliminacji zagrożeń

5.1. Obliczanie wartości współczynników cyfrowego cienia zestawu czujników

Dana jest siatka czujników o wymiarach 3×4, mierzących pewną wielkość. Czujniki wysyłają zmierzone wartości w chwilach t_k do brzegowej stacji bazowej (rys. 1). W symulacji wykonanej w środowisku obliczeniowym MATLAB przyjęto, że w wyniku kolejnych pięciu pomiarów w chwilach t_1, t_2, ..., t_5 otrzymano zbiór wartości danych $[c_{ij}]$, uzyskanych przez sumowanie wartości deterministycznych i losowych, generowanych funkcją *randn*().



Rys. 1. Sieć czujników i graniczna stacja bazowa
Fig. 1. Sensor network and border base station

5.1.1. Wyznaczanie wartości współczynników cyfrowego cienia zestawu czujników mierzących wartości stabilne

Dane pomiarowe są zapisywane w macierzy trójwymiarowej, w której pierwsze dwa wymiary odpowiadają wymiarom siatki, a trzeci wymiar odzwierciedla liczbę chwil, w których wykonano te pomiary. Przykładowe dane są zestawione w tabeli 1.

Tab. 1. Zbiór danych
Tab. 1. Data set

t_k	Wartości c_{ij}			
t_1	10,017	9,051	7,881	6,935
	9,035	8,005	7,079	5,845
	8,017	7,006	6,120	4,920
t_2	9,895	8,925	8,094	6,873
	9,050	7,721	7,073	6,077
	7,916	6,887	6,142	5,072
t_3	9,922	8,968	8,141	6,960
	8,907	7,839	6,934	6,214
	8,054	7,154	5,980	5,050
t_4	9,962	9,041	7,959	6,964
	8,940	8,059	7,085	6,185
	8,021	7,027	6,065	5,048
t_5	9,993	9,094	8,016	7,027
	9,041	7,929	6,994	5,815
	7,960	7,054	5,909	4,935

Tab. 2. Błędy procentowe wartości c_{ij}^*
Tab. 2. Percentage errors of values c_{ij}^*

0,22 %	−0,73 %	−1,63 %	6,60 %
0,48 %	2,47 %	−2,64 %	3,15 %
−1,26 %	−0,08 %	3,11 %	−1,53 %

W wyniku rozwiązania odpowiednich układów równań (4) otrzymuje się cyfrowy cień zestawu czujników, w którym wektory $[\alpha_{uv}]$ wynoszą odpowiednio:
— dla czujników narożnych:

$$[\alpha_{11}] = \begin{bmatrix} 0,9911 \\ 0,1159 \end{bmatrix}, \quad [\alpha_{14}] = \begin{bmatrix} 3,3683 \\ -3,3549 \end{bmatrix},$$

$$[\alpha_{31}] = \begin{bmatrix} 0,2108 \\ 0,8725 \end{bmatrix}, \quad [\alpha_{34}] = \begin{bmatrix} 0,1978 \\ 0,6346 \end{bmatrix};$$

— dla pozostałych czujników na brzegu siatki:

$$[\alpha_{12}] = \begin{bmatrix} 0,7173 \\ 0,0581 \\ 0,1758 \end{bmatrix}, \quad [\alpha_{13}] = \begin{bmatrix} -3,9905 \\ 5,1242 \\ 1,3823 \end{bmatrix},$$

$$[\alpha_{21}] = \begin{bmatrix} 2,1489 \\ -0,8979 \\ -0,6612 \end{bmatrix}, \quad [\alpha_{24}] = \begin{bmatrix} -0,9072 \\ 0,5513 \\ 1,7163 \end{bmatrix},$$

$$[\alpha_{32}] = \begin{bmatrix} 1,4079 \\ -0,1235 \\ -0,5380 \end{bmatrix}, \quad [\alpha_{33}] = \begin{bmatrix} -0,1226 \\ 0,9218 \\ 0,0920 \end{bmatrix};$$

— dla czujników wewnętrznych siatki:

$$[\alpha_{22}] = \begin{bmatrix} -1,0740 \\ 2,9626 \\ -0,4493 \\ -0,8454 \end{bmatrix}, \quad [\alpha_{23}] = \begin{bmatrix} 0,1241 \\ -0,2173 \\ 0,2192 \\ 1,0648 \end{bmatrix}.$$

Błędy procentowe wyznaczonych dla cieni czujników wartości c_{ij}^*, obliczone z zależności $\left(c_{ij}^* - c_{ij}\right) / c_{ij} \cdot 100\ \%$ są zestawione w tabeli 2, a ich wartości bezwzględne wahają się od 0,08 % do 6,60 %.

Biorąc pod uwagę dokładność pomiarów, która jest zwykle rzędu kilku procent, można przyjąć, że próg 10 % różnicy między wartością cienia a wartością zmierzoną jest podstawą do wygenerowania alarmu o możliwej awarii lub przejęciu czujnika; alarm ten może być również skutkiem nietypowego zdarzenia, np. punktowego zakwaszenia gleby.

5.1.2. Wyznaczanie wartości współczynników cyfrowego cienia zestawu czujników mierzących wartości narastające mierzonej wielkości

Dla zbioru danych z tabeli 3, po obliczeniu wektorów $[\alpha_{uv}]$ wartości błędów procentowych wyznaczonych dla cieni czujników c_{ij}^*, obliczone z zależności $\left(c_{ij}^* - c_{ij}\right) / c_{ij} \cdot 100\ \%$ są zestawione w tabeli 4, a ich wartości bezwzględne wahają się od 0,19 % do 3,82 %.

Tab. 3. Zbiór danych
Tab. 3. Data set

t_k	Wartości c_{ij}			
t_1	11,008	10,095	9,041	7,932
	10,914	9,931	8,955	8,010
	11,083	9,946	9,090	8,013
t_2	12,015	11,101	10,212	8,950
	11,873	11,038	10,065	8,917
	12,101	10,953	9,986	8,971
t_3	13,030	11,960	10,907	10,018
	13,213	12,115	11,063	9,880
	12,975	12,143	10,998	10,056
t_4	13,782	13,114	12,250	11,044
	13,860	13,026	12,016	10,925
	14,027	13,158	12,048	11,033
t_5	15,066	13,991	13,088	11,968
	15,078	13,819	12,814	11,940
	15,010	13,944	13,011	12,090

Tab. 4. Błędy procentowe wartości c^*_{ij}
Tab. 4. Percentage errors of values c^*_{ij}

−1,60 %	0,19 %	−2,79 %	−3,82 %
1,36 %	1,40 %	0,37 %	−2,28 %
2,46 %	3,37 %	−2,76 %	0,46 %

W obu przeanalizowanych przykładach wartości błędów delta*e* są mniejsze od przyjętego progu 10 % jako wartości, której przekroczenie generuje alarm.

W celu zilustrowania eliminacji wybranych ataków zaprezentowano dalej przykład obliczeniowy na podstawie danych z pkt. 5.1.1.

5.2. Eliminacja utraty danych z czujnika

Niezależnie od przyczyny (losowej awarii czy też ataku intruza), jeżeli w BS zostanie wykryta utrata danych z czujnika c_{ij}, tj. $c_{ij} = 0$, cyfrowy cień w pierwszym kroku wylicza wartość c^*_{ij}, a w kolejnych krokach oblicza pozostałe wartości dla cieni poszczególnych czujników z uwzględnieniem wartości cienia i odpowiednie błędy procentowe.

Dla przykładu, jeżeli nastąpiła utrata danych dla c_{22}, tj. $c_{22} = 0$, cyfrowy cień wyznaczył wartość $c^*_{22} = 8{,}1245$ i odpowiednie wartości błędów, zestawione w tabeli 5:

Tab. 5. Błędy procentowe wartości c^*_{ij}
Tab. 5. Percentage errors of values c^*_{ij}

0,22 %	−0,35 %	−1,63 %	6,60 %
−0,95 %	0,00 %	−2,29 %	3,15 %
1,26 %	−0,42 %	3,11 %	−1,53 %

Porównując dane w tabelach 2 i 5 można zauważyć, że dla czujnika c_{22} wyliczona wartość jest wartością cienia, gdyż błąd wynosi 0,00 %, wartości błędów dla tych czujników, dla których wartość cienia nie była zależna od wartości c_{22} nie uległy zmianie, natomiast uległy zmianie wartości obliczone dla cieni czujników sąsiadujących bezpośrednio z czujnikiem c_{22}. Jeżeli, jak w analizowanym przykładzie, błędy te nie przekroczyły wartości przyjętej za graniczną, to zastosowane rozwiązanie umożliwia prawidłową pracę układu oraz podjęcie działań mających na celu ustalenie i usunięcie przyczyn, które wywołały utratę danych z czujnika.

5.3. Wykrywanie sfałszowanych danych z czujnika lub wykrywanie anomalii

Jeżeli wartość bezwzględna obliczonego błędu procentowego dla czujnika c_{ij} przekracza wartość graniczną, BS zgłasza alarm i – w zależności od przyjętej polityki – wyznacza wartość sterowań dla aktuatorów na podstawie wartości obliczonej dla cienia c^*_{ij} albo na podstawie zmierzonej wartości lub wartości historycznych. Polityka może oczywiście przewidywać różne ścieżki zachowania się układu po wykryciu takiego stanu, w zależności od sterowanego układu, w szczególności na podstawie znajomości jego dynamiki, wartości stwierdzonej odchyłki, krotności wystąpienia odchyłki itp.

Przykład

Niech $c_{11} = 12$, co oznacza odchyłkę od wartości wyznaczonej przez cień o około 20 %, a zatem przekracza ustalony w przykładzie próg 10 %.

Obliczone błędy procentowe obliczonych wartości cienia w porównaniu do wartości zmierzonych są zestawione w tabeli 6 i wskazują, że zaatakowanym węzłem jest czujnik c_{11}, który przesłał wartość przekraczającą przyjęty próg błędów i „zatruwa" wartości c_{12} i c_{22}. Zarówno c_{13}, jak i c_{21} nie są węzłami toksycznymi, gdyż błędy procentowe dla ich sąsiadów nie przekraczają ustalonego progu.

Tab. 6. Błędy procentowe wartości c^*_{ij}
Tab. 6. Percentage errors of values c^*_{ij}

−16,54 %	15,10 %	−1,63 %	6,60 %
48,18 %	2,47 %	−2,64 %	3,15 %
1,26 %	−0,08 %	3,11 %	−1,53 %

Tab. 7. Błędy procentowe wartości c^*_{ij}
Tab. 7. Percentage errors of values c^*_{ij}

0,22 %	−0,73 %	−1,63 %	6,60 %
0,48 %	2,47 %	−2,64 %	3,15 %
1,26 %	−0,08 %	3,11 %	−1,53 %

Jeżeli zamiast przesłanej wartości zmierzonej przez czujnik c_{11} (lub wartości sfalsyfikowanej w transmisji) zostanie przyjęta wartość cienia $c^*_{11} = 10{,}0146$, to wówczas wartości błędów procentowych, jak pokazano w tab. 7, mieszczą się w granicach tolerancji i układ pracuje poprawnie.

5.4. Eliminacja podstawienia fałszywego czujnika

Eliminacja podstawienia fałszywego czujnika jest możliwa zarówno wtedy, gdy intruz zastępuje autentyczny czujnik czujnikiem fałszywym (przypadek a), jak i na skutek dodania do sieci czujników czujnika fałszywego (przypadek b).

W przypadku (a) wykrycie ataku zamiany czujnika jest tożsame z wykryciem opisanych w pkt. 5.3. danych sfałszowa-

nych. W przypadku (b) wykrycie następuje przez porównanie danych otrzymanych przez BS ze zbiorem stanów dopuszczalnych urządzeń IoT opisanym w pracy [19]. Wskazany tam zbiór stanów pożądanych Z* może zawierać tylko takie elementy, w których ocena stanu bezpieczeństwa jest ustalona jako prawidłowa lub też takie elementy, dla których stany pracy przyjmują wyznaczone wartości, a zatem w szczególności znaną *a priori* listę czujników, dla których wartości zmierzone muszą zawierać się w określonym przedziale wartości.

6. Podsumowanie

Jak wynika z przeprowadzonej analizy, zaprezentowana propozycja wykorzystania macierzowego cyfrowego cienia sieci czujników IoT pozwala na ocenę prawidłowości pracy takiej sieci w czasie rzeczywistym od momentu zakończenia procesu tworzenia pierwszej wersji cienia, a zatem pierwszego cyklu „uczenia się" układu BS. Czas trwania procesu „uczenia się" zależy od przyjętego typu ε_k – sąsiedztwa, wymaga zapamiętania macierzy $\mathbf{B}_{m\times n\times p}$ zawierającej co najmniej 4k albo 8k kolejnych wartości zmierzonych przez czujniki oraz wyznaczenia wartości wektorów $[\alpha_{uv}]$ albo $[\alpha_{uv}]$ i $[\beta_{wz}]$. Proces wyznaczania wektorów współczynnika cienia powinien być ponawiany po każdym kolejnym odczycie wartości zmierzonych przez czujniki, jeśli ten odczyt zostanie uznany za prawidłowy. Proces uczenia się obejmuje również wprowadzenie do układu BS macierzy opisującej stany pożądane monitorowanej sieci czujników.

Jeżeli w macierzy delta$e$ wartości błędów procentowych przekraczałyby arbitralnie przyjęty próg akceptowalnych wartości błędów delta$e$, wówczas układ BS może podjąć decyzję, czy przyczyną jest utrata danych z czujnika albo falsyfikacja tych danych, a na podstawie porównania z macierzą stanów pożądanych – wykrycie podstawienia fałszywego, dodatkowego czujnika.

Ze względu na obliczanie wartości wektorów $[\alpha_{uv}]$ i $[\beta_{wz}]$ metodą rozwiązywania układów równań liniowych, proponowany proces może być stosowany wtedy, gdy odpowiednie macierze są nieosobliwe i na dokładność obliczeń nie ma istotnego wpływu ich ewentualne złe uwarunkowanie [20].

Wymagane dla zastosowania proponowanego cyfrowego cienia niewielkie zasoby pamięci i mocy obliczeniowej układu BS są niewątpliwą zaletą takiego rozwiązania, podnoszącego bezpieczeństwo pracy sieci czujników i układu BS wyznaczającego wartości sygnałów sterujących dla urządzeń wykonawczych.

Bibliografia

1. Faris M., Mahmud M.N., Salleh M.F.M., Alnoor A., *Wireless sensor network security: A recent review based on state-of-the-art works*, "International Journal of Engineering Business Management", 2023, DOI: 10.1177/18479790231157220.
2. Jabeen T., Jabeen I., Ashraf H., Jhanjhi N.Z., Yassine A., Hossain M.S., *An Intelligent Healthcare System Using IoT in Wireless Sensor Network*, "Sensors", Vol. 23, No. 11, 2023, DOI: 10.3390/s23115055.
3. Ahmad R., Wazirali R., Abu-Ain T., *Machine Learning for Wireless Sensor Networks Security: An Overview of Challenges and Issues*, "Sensors", Vol. 22, No. 13, 2022, DOI: 10.3390/s22134730.
4. Schiller E., Aidoo A., Fuhrer J., Stahl J., Ziörjen M., Stiller B., *Landscape of IoT security*, "Computer Science Review", Vol. 44, 2022, DOI: 10.1016/j.cosrev.2022.100467.
5. Gelernter D., *Mirror Worlds*, Oxford University Press, 1993.
6. Glaessgen E., Stargel D., *The Digital Twin Paradigm for Future NASA and U.S. Air Force Vehicles*, DOI: 10.2514/6.2012-1818.
7. Singh S., Weeber M., Birke K.-P., *Advancing digital twin implementation: a toolbox for modelling and simulation*, "Procedia CIRP", Vol. 99, 2021, 567–572, DOI: 10.1016/j.procir.2021.03.078.
8. Kritzinger W., Karner M., Traar G., Henjes J., Sihn W., *Digital Twin in manufacturing: A categorical literature review and classification*, "IFAC-PapersOnLine", Vol. 51, No. 11, 2018, 1016–1022, DOI: 10.1016/j.ifacol.2018.08.474.
9. Singh M., Fuenmayor E., Hinchy E.P., Qiao Y., Murray N., Devine D., *Digital Twin: Origin to Future*, "Applied System Innovation", Vol. 4, No. 2, 2021, DOI: 10.3390/asi4020036.
10. Grzesik W., *Cyfrowy bliźniak w procesach wytwórczych Część I. Stan zagadnienia, architektura i zastosowania*, "Mechanik", No. 1, 2023, 8–13, DOI: 10.17814/mechanik.2023.1.1.
11. Grieves M., *Digital Model, Digital Shadow, Digital Twin*. Preprint, 2023.
12. Shao G., Frechette S., Srinivasan V., *An Analysis of the New ISO 23247 Series of Standards on Digital Twin Framework for Manufacturing*, MSEC Manufacturing Science & Engineering Conference 2023, New Brunswick, New Jersey, USA, [https://tsapps.nist.gov/publication/get_pdf. cfm?pub_id=935765].
13. Fragkiadakis A., Angelakis V., Tragos E.Z., *Securing Cognitive Wireless Sensor Networks: A Survey*, "International Journal of Distributed Sensor Networks", Vol. 10, No. 3, 2014, DOI: 10.1155/2014/393248.
14. Iwaniec W., *Ochrona urządzeń Internetu Rzeczy* (*IoT*) *na brzegu sieci lokalnej*, [W:] Krzyńska-Nawrocka E. (red.): „Innowacje i inspiracje. 150-lecie urodzin Jana Szczepanika", 2022, Tarnów, Wydawnictwa PWSZ w Tarnowie, 81–93, ISBN 978-83-963518-5-2 2022-12.
15. Jaroś K., *Sterowanie predykcyjne i fuzja danych w systemie dynamicznego pozycjonowania statku*, rozprawa doktorska, Politechnika Gdańska 2023.
16. Chen G., Liu Z., Yu G., Liang J., *A new view of multisensor data fusion: Research on generalized fusion*. "Mathematical Problems in Engineering", 2021, DOI: 10.1155/2021/5471242.
17. Veysi P., Adeli M., Naziri N.P., Adeli E., *A Gentle Approach to Multi-Sensor Fusion Data Using Linear Kalman Filter*, "Computers and Society", 2024, DOI: 10.48550/arXiv.2407.13062.
18. Urrea C., Agramonte R. *Kalman Filter: Historical Overview and Review of Its Use in Robotics 60 Years after Its Creation*, "Journal of Sensors", 2021, DOI: 10.1155/2021/9674015.
19. Iwaniec W., *Identyfikacja zagrożeń w macierzowym modelu stanu pracy i bezpieczeństwa urządzeń IoT*, „Pomiary Automatyka Robotyka", R. 24, Nr 1, 2020, 67–74, DOI: 10.14313/PAR_235/67.
20. Mitkowski W., *Równania macierzowe i ich zastosowania*. Wyd. drugie poprawione, Wydawnictwa AGH, Kraków 2007.

Inne źródła

21. Bauernhans T., Krüger J., Reinhart G., Schuh G., *WGP-Standpunkt Industrie 4.0*, Darmstadt, 2016, [https://wgp.de/wp-content/uploads/WGP-Standpunkt_Industrie_4-0.pdf].

22. *Digital Twins for Advanced Manufacturing*, [www.nist.gov/programs-projects/digital-twins-advanced-manufacturing].
23. ISO 23247-1:2021(en) *Automation systems and integration — Digital twin framework for manufacturing — Part 1: Overview and general principles*, https://www.iso.org/obp/ui/#iso:std:iso:23247:-1:ed--1:v1:en.
24. White F.E., *Data Fusion Lexicon*, Defense Technical Information Center, 1991.

Matrix Digital Shadow of IoT Sensors Network

Abstract: This paper presents the concept of a matrix digital shadow of an IoT sensor network. The differences between digital twin and digital shadow are discussed and the choice of the sensor network shadow concept is justified. A matrix description of such a network is presented and the concept of ε_k – neighborhood of sensor is introduced. Formulas for linear models of plus and star ε_k – neighborhoods are provided. Selected examples show the possibility of detecting and eliminating some security threats to sensor networks.

Keywords: digital shadows, Internet of Things security, IoT device security threats, sensors networks, matrix models

dr inż. Władysław Iwaniec
wiw@atar.edu.pl
ORCID: 0000-0002-5253-7710

Adiunkt w Katedrze Automatyki i Robotyki Akademii Tarnowskiej w Tarnowie, w której był prorektorem w latach 1998–2007. Ma bogate doświadczenie w zakresie wdrażania i eksploatacji systemów informatycznych. Pracował m.in. jako dyrektor Ośrodka Informatyki Urzędu Wojewódzkiego w Tarnowie, brał udział w wielu przedsięwzięciach z zakresu zastosowań informatyki w służbie zdrowia, uczestniczył w organizacji obsługi informatycznej wyborów na szczeblu krajowym i okręgowym. Odznaczony m.in. Złotym Krzyżem Zasługi i Srebrnym Medalem za „Zasługi dla obronności kraju". Zainteresowania naukowe obejmują zagadnienia kryptografii i bezpieczeństwa sieci i systemów komputerowych oraz identyfikacji układów sterowania.