

MACIERZOWY CYFROWY CIEŃ BEZPRZEWODOWYCH SIECI CZUJNIKÓW IOT

Władysław Iwaniec
wiw@atar.edu.pl

Akademia Tarnowska, ul. Mickiewicza, 33-100 Tarnów

Streszczenie

Systemy IoT i sieci WSN znajdują obecnie różnorodne zastosowania, wpływając na niemal każdy obszar działalności człowieka, od środowiska i flory oraz fauny, po przemysł i opiekę zdrowotną [1] [2].

W wielu artykułach naukowych podkreśla się znaczenie ataków na czujniki dla bezpieczeństwa systemów monitorowania i sterowania. Ważną metodą poprawy bezpieczeństwa sieci czujników jest tworzenie cyfrowego cienia takiej sieci.

W artykule [3] 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. Zgodnie z rozwiązaniem zaproponowanym w [4] zakłada się, że czujniki nie komunikują się bezpośrednio ze sobą, lecz przesyłają wszystkie dane do urządzenia brzegowego BS (topologia gwiazdy, rys. 1). Zbiór wartości zmierzonych

w danej chwili t przez zbiór tych czujników można opisać macierzą: gdzie c_{ij} oznacza wartość zmierzoną przez czujnik ij w danej chwili t .

$$C_{mn}^t = \begin{bmatrix} c_{11} & c_{12} & c_{13} & \cdots & c_{1n} \\ c_{21} & c_{22} & c_{23} & \cdots & c_{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_{m1} & c_{m2} & c_{m3} & \cdots & c_{mn} \end{bmatrix}, \quad (1)$$

Wtedy wartość cienia c_{ij}^* wartości mierzonej przez czujnik c_{ij} można wyrazić w liniowym modelu ε_k -sąsiedztwa wzorem:

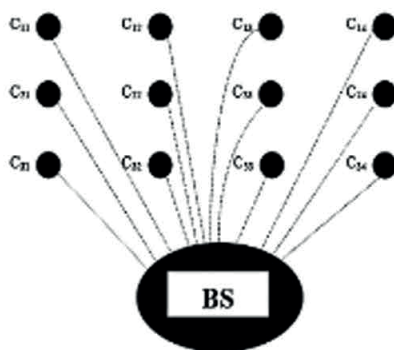
$$c_{ij}^* = [\alpha_{uv}] \cdot [c_{uv}]^T, \quad (2)$$

gdzie:

$$[\alpha_{uv}] = [\alpha_{i-kj}, \alpha_{i-(k-1)j}, \dots, \alpha_{i-1j}, \alpha_{ij-k}, \alpha_{ij-(k-1)}, \dots, \alpha_{ij-1}, \alpha_{i+1j}, \dots, \alpha_{i+(k-1)j}, \alpha_{i+kj}, \alpha_{i+j+1}, \dots, \alpha_{i-j+(k-1)}, \alpha_{ij+k}],$$

$$[c_{uv}] = [c_{i-kj}, c_{i-(k-1)j}, \dots, c_{i-1j}, c_{ij-k}, c_{ij-(k-1)}, \dots, c_{ij-1}, c_{i+1j}, \dots, c_{i+(k-1)j}, c_{i+kj}, c_{ij+1}, \dots, c_{ij+(k-1)}, c_{ij+k}],$$

$$|i-u| \leq k, |j-v| \leq k.$$



Rys.1. Sieć czujników i graniczna stacja bazowa.

Fig.1. Sensor network and border base station

Wartości współczynników $[\alpha_{uv}]$ można wyznaczyć przez rozwiązanie układu 4-k równań liniowych. Dla zastosowania tej metody konieczne jest „uczenie maszynowe” BS przez co najmniej 4-k cykle pomiarowe. W pracy [4] wykazano, że

metoda ta umożliwia wykrywanie ataków i uszkodzeń czujników.

Analiza środowiska (np. [5]), w którym pracują czujniki wykazuje, że celowe jest rozszerzenie modelu liniowego na model wielomianowy. Taki model opisany jest wzorem:

$$c_{ij}^* = [\alpha_{uv}^{(1)}] \cdot [c_{uv}]^T + [\alpha_{uv}^{(2)}] \cdot [c_{uv}^2]^T + \dots + [\alpha_{uv}^{(r)}] \cdot [c_{uv}^r]^T \quad (3)$$

gdzie:

$[\alpha_{uv}^{(s)}]$ jest wektorem współczynników cienia dla s-tej potęgi wartości zmierzonych przez sąsiednie czujniki, $[c_{uv}^s]$ jest wektorem s-tych potęg wartości zmierzonych przez sąsiednie czujniki, $s=1,2,\dots,r$.

Dla obliczenia wartości wektorów $[\alpha_{uv}^{(s)}]$ konieczne jest rozwiązanie układu 4-k-s równań liniowych.

Dla zastosowania tej metody konieczne jest „uczenie maszynowe” BS przez co najmniej 4-k-s cykli pomiarowych. Celowe jest tworzenie cienia WSN dla kolejnych wartości $s=1,2,\dots$, aż do uzyskania wymaganej dokładności. Zaletą krokowego tworzenia cyfrowych cieni jest możliwość wykrywania anomalii już po pierwszym kroku.

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

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

Bibliografia/References

- [1] Kandris. D., Nakas. C., Vomvas. D., Koulouras.G., Applications of Wireless Sensor Networks: An Up-To-Date Survey. Applied System Innovation 2020, 3, 14. doi.org/10.3390/asi3010014
- [2] Kandris D., Anastasiadis E., Advanced Wireless Sensor Networks: Applications, Challenges and Research Trends, Electronics 2024, 13(12), 2268; doi.org/10.3390/electronics13122268
- [3] Iwaniec W., Macierzowy cyfrowy cień sieci czujników IoT, „Pomiary Automatyka Robotyka”, R. 29, Nr 1/2025, 91-97, DOI: 10.14313/PAR_255/91.
- [4] 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.
- [5] Zieliński T. Zagrożenia i przeciwdziałanie bezzałogowym statkom powietrznym w ochronie portów lotniczych, Rocznik Bezpieczeństwa Morskiego, Rok XVI-2022, doi:10.5604/01.3001.0016.1915

MATRIX DIGITAL SHADOW OF IOT WIRELESS SENSORS NETWORK

Władysław Iwaniec
wiw@atar.edu.pl

Akademia Tarnowska, ul. Mickiewicza , 33-100 Tarnów

The IoT systems and WSNs now have various applications impacting nearly every area of human activity, ranging from the environment and flora and fauna, to industry and healthcare [1] [2].

Many research papers highlight the importance of attacks on sensors, for the security of monitoring and control systems. An important method for improving the security of sensor networks is to create a digital shadow of such a network. In paper [3] the differences between digital twin and digital shadow are discussed and the choice of the

sensor network shadow concept is justified. According to the solution proposed in [4], it is assumed that sensors nodes do not communicate directly one with other, they send all data to the Border Station (star topology, Fig. 1). The set of values measured at a given time moment t by the set of these sensors can be written as a matrix:

$$C_{m \times n}^t = \begin{bmatrix} c_{11} & c_{12} & c_{13} & \cdots & c_{1n} \\ c_{21} & c_{22} & c_{23} & \cdots & c_{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_{m1} & c_{m2} & c_{m3} & \cdots & c_{mn} \end{bmatrix}, \quad (1)$$

where c_{ij} denotes the value measured by sensor i,j at a given time t .

Then the shadow value c_{ij}^* of the value measured by the sensor c_{ij} can be expressed in the linear ε_k -neighborhood model by the formula:

$$c_{ij}^* = [\alpha_{uv}] \cdot [c_{uv}]^T, \quad (2)$$

where:

$$[\alpha_{uv}] = [\alpha_{i-kj}, \alpha_{i-(k-1)j}, \dots, \alpha_{i-1j}, \alpha_{ij-k}, \alpha_{ij-(k-1)}, \dots, \alpha_{ij-1}, \alpha_{i+1j}, \dots, \alpha_{i+(k-1)j}, \alpha_{i+kj}, \alpha_{i+j+1}, \dots, \alpha_{ij+(k-1)}, \alpha_{ij+k}],$$

$$[c_{uv}] = [c_{i-kj}, c_{i-(k-1)j}, \dots, c_{i-1j}, c_{ij-k}, c_{ij-(k-1)}, \dots, c_{ij-1}, c_{i+1j}, \dots, c_{i+(k-1)j}, c_{i+kj}, c_{ij+1}, \dots, c_{ij+(k-1)}, c_{ij+k}],$$

$$|i - u| \leq k, |j - v| \leq k.$$

The values of the coefficients $[\alpha_{uv}]$ can be calculated by solving a system of $4k$ linear equations. To apply this method, it is necessary to „machine learning” the BS for at least $4 \cdot k$ measurement cycles. In [4] it has been shown that this method makes it possible to detect of at-

tacks and sensor damage.

Analysis of the environment (e.g.[5]) in which the sensors operate shows that it is advisable to extend the linear model to a polynomial model. Such a model is described by the formula:

$$c_{ij}^* = [\alpha_{uv}^{(1)}] \cdot [c_{uv}]^T + [\alpha_{uv}^{(2)}] \cdot [c_{uv}^2]^T + \dots + [\alpha_{uv}^{(r)}] \cdot [c_{uv}^r]^T \quad (3)$$

here:

$[\alpha_{uv}^{(s)}]$ is the vector of shadow coefficients for the s -th power of the values measured by neighboring sensors, $[c_{uv}^s]$ is the vector of s -th powers of the values measured by neighboring sensors,

$s = 1, 2, \dots, r$.

To calculate the values of the vectors $[\alpha_{uv}^{(s)}]$ it is necessary to solve

the system of $4 \cdot k \cdot s$ linear equations. To apply this method, it is necessary to „machine learning” the BS for at least $4 \cdot k \cdot s$ measurement cycles. It is advisable to create a WSN shadow for subsequent values of $s=1, 2, \dots$, until the required accuracy is achieved. The advantage of step-by-step digital shadow creation is the ability to detect anomalies after the first step.