DOI: https://doi.org/10.15276/ict.01.2024.13
УДК 004.75

Модуль вразливості у багаторівневій онтології оцінки ризиків бездротової сенсорної мережі

Штільман Павло Романович[1)]
Аспірант, каф. Комп'ютерні інтелектуальні системи та мережи
ORCID: https://orcid.org/0009-0007-8061-1766; pavel52shtilman62@gmail.com
Тішин Петро Метталинович[1)]
Канд. математичних наук, каф. Комп'ютерні інтелектуальні системи та мереж
ORCID: https://orcid.org/0000-0003-2506-5348; petrmettal@gmail.com. Scopus Author ID: 57190400970
[1)] Національний університет «Одеська політехніка», пр. Шевченка, 1. Одеса, 65044, Україна

АНОТАЦІЯ

У цій роботі представлено розробку модуля вразливості в межах багаторівневої онтології для оцінки ризиків у бездротових сенсорних мережах, що використовуються в промислових середовищах. БСМ складаються з декількох сенсорних вузлів з мікроконтролерами, датчиками, пристроями передачі даних та джерелами живлення, і відіграють ключову роль у моніторингу, діагностиці та управлінні виробничими процесами. Основними перевагами БСМ є зниження витрат завдяки відсутності необхідності прокладання кабелів та легкість масштабування шляхом додавання нових вузлів. Однак, БСМ стикаються з низкою проблем, зокрема обмеженістю джерел живлення, вразливістю до електромагнітних перешкод, низькою пропускною здатністю та загрозами кіберзлому. Ці проблеми роблять їх менш придатними для систем реального часу, де критично важлива швидкість і надійність передачі даних. Модуль вразливості, розроблений у рамках цього дослідження, допомагає вирішити ці виклики, ідентифікуючи слабкі місця, аналізуючи потенційні загрози та оцінюючи ризики за допомогою логічних правил. Ці правила оцінюють різні компоненти мережі, такі як пристрої, протоколи зв'язку та зовнішні фактори, наприклад фізичний доступ і радіоінтерференції. Модуль постійно моніторить мережу, виявляє нові вразливості та надає зворотний зв'язок у режимі реального часу до модуля оцінки ризиків, пропонуючи заходи щодо зменшення ризиків. Це підвищує безпеку та надійність БСМ у промислових застосуваннях. На завершення, модуль вразливості в межах багаторівневої онтології забезпечує структурований підхід до виявлення та усунення ризиків у БСМ. Незважаючи на внутрішні вразливості БСМ, вдосконалення протоколів безпеки та енергоефективності роблять їх дедалі більш придатними для автоматизації та оптимізації промислових процесів.

Ключові слова: Бездротові сенсорні мережі (БСМ); вразливості; оцінка ризиків; промислові системи; логічні правила; безпека мережі; кіберзагрози; енергоефективність; модуль вразливості; мережеві протоколи; автоматизація промисловості; загрози інформаційної безпеки; онтологія; Web Ontology Language (OWL)

Бездротові сенсорні мережи (БСМ) – це розподілені мережі, які складаються з декількох сенсорних вузлів, кожен з яких містить мікроконтролер, датчики, пристрій передачі даних та джерело живлення. Основними задачами цих вузлів як єдиний пристрій є збір, обробка та передача даних який він збирає від зони спостереження у режимі реального часу.

Актуальність. Важливість дослідження модуля вразливості у багаторівневій онтології оцінки ризиків бездротових сенсорних мереж (БСМ) зумовлена їхнім широким впровадженням у різні сфери нашої життєдіяльності, зокрема в промисловість. БСМ у промисловості використовуються для:

- спостереження виробничих процесів;
- контролю виробничих систем;
- діагностики обладнання;
- керування активами та виробничими операціями.

Проте такі мережі мають низку проблем, включаючи обмежене енергоспоживання, електромагнітні перешкоди, низьку пропускну здатність і вразливість до кіберзагроз, що ставить під загрозу їхню надійність і безпеку. Розробка модуля, який здатен виявляти й усувати вразливості БСМ, є важливою для забезпечення стабільної та безпечної роботи цих мереж у промислових умовах.

Мета дослідження — створення модуля вразливості БСМ. Даний модуль передбачає створення незбагаченої системи логічних співвідношень, яка описує параметри та невідомі змінні, вхідні в модуль уразливості БСМ. Кожне логічне співвідношення має змістовні

This is an open access article under the CC BY license (https://creativecommons.org/licenses/by/4.0/deed.uk)

тлумачення, а вся система загалом поглиблюється у поданні концептуалізації, яка розуміється як множина ситуацій та множини систем знань у конкретній галузі.

У дослідженні модуля вразливості в багаторівневій онтології оцінки ризиків для бездротових сенсорних мереж (БСМ), представленому в документі, акцент робиться на аналізі слабких місць БСМ у промислових середовищах і пропонується підхід для їх усунення за допомогою логічних правил. Якщо порівнювати це дослідження з іншими статтями зі списку:

У роботі [1], яка зосереджується на багаторівневій онтології ризиків, надає корисний контекст для використання методології CORAS для оцінки вразливостей, що тісно пов'язано з запропонованим модулем вразливості, але її фокус більше на загальних ризиках, ніж на технічних аспектах БСМ. Робота [2] підходить для загального огляду бездротових мереж у промисловій автоматизації, але не надає детального аналізу вразливостей чи загроз, що є основою для поточного дослідження. У роботі [3] запропонована система динамічного виявлення подій у БСМ, що є корисним доповненням, оскільки вона акцентує увагу на обробці подій у реальному часі, але не дає комплексного аналізу ризиків і вразливостей. Роботи [4] і [5], що розглядають архітектуру і онтології атак, надають важливу основу для розуміння протоколів і потенційних загроз у БСМ, але не включають практичних методів для виявлення і мінімізації ризиків, як це робиться в модулі вразливості. Статті [6] і [7], що фокусуються на промисловому моніторингу та оптимізації мереж, є більш практичними, але не надають глибокого аналізу безпеки. Стаття [8] з онтологією семантичних сенсорних мереж корисна для моделювання мережевих взаємодій, однак вона не висвітлює питання безпеки. У порівнянні зі статтею [9], яка розглядає моніторинг залізничної інфраструктури, цей модуль вразливості має більше технічних деталей щодо виявлення загроз. Робота [10] розглядає інновації в мережах, що робить її корисною для майбутніх напрямків, але модуль вразливості надає вже готові рішення для поточних проблем. Стаття [11] зосереджується на гетерогенних БСМ, що важливо для управління складними мережами, але менше уваги приділяється безпеці.

Таким чином, цей модуль вразливості є вагомим доповненням до існуючих досліджень у сфері БСМ, зосереджуючись на реальних загрозах і практичних методах їх усунення, що робить його особливо корисним у промислових застосуваннях.

Перевагами БСМ над звичайними системами є значне зниження затрат при установці чи обслуговуванні, завдяки відсутності необхідності прокладання кабельних трас. Це також вирішує проблему із прокладанням кабельних трас в особо складних чи небезпечних умовах через різні побічні промислові або природні явища. Іншою перевагою БСМ є легке масштабування, це дозволяє швидко додавати нові вузли та розширювати систему без необхідності внесення змін до фізичної інфраструктури промислового об’єкта. Це є доволі актуальним при необхідності збільшення виробничої лінії.

До основних вразливостей БСМ у промислових умовах належать обмежена автономність через використання акумуляторів, що зменшує тривалість роботи та ускладнює обслуговування вузлів у важкодоступних місцях. Також присутні електромагнітні перешкоди, які можуть негативно впливати на роботу мережі, особливо в умовах щільної забудови та наявності металевих поверхонь. Обмежена пропускна здатність і затримки передачі даних роблять БСМ непридатними для систем із вимогами реального часу. Додатковою проблемою є інформаційна безпека, оскільки БСМ уразливі до перехоплення даних і кібератак через обмеженість ресурсів для реалізації складних криптографічних алгоритмів.

Незважаючи на існуючи недоліки або вразливості БСМ мають значний потенціал для використання у промисловій автоматизації. Розвиток енергоємних акумуляторів, нових технологій енергоефективності, вдосконалення протоколів передачі даних, а також розробка більш захищених систем зв’язку можуть дозволити зробити БСМ більш затребуваними.

Розроблений підхід передбачає створення багаторівневої моделі онтології, як сукупності модулів, яка представлена на рис. 1.

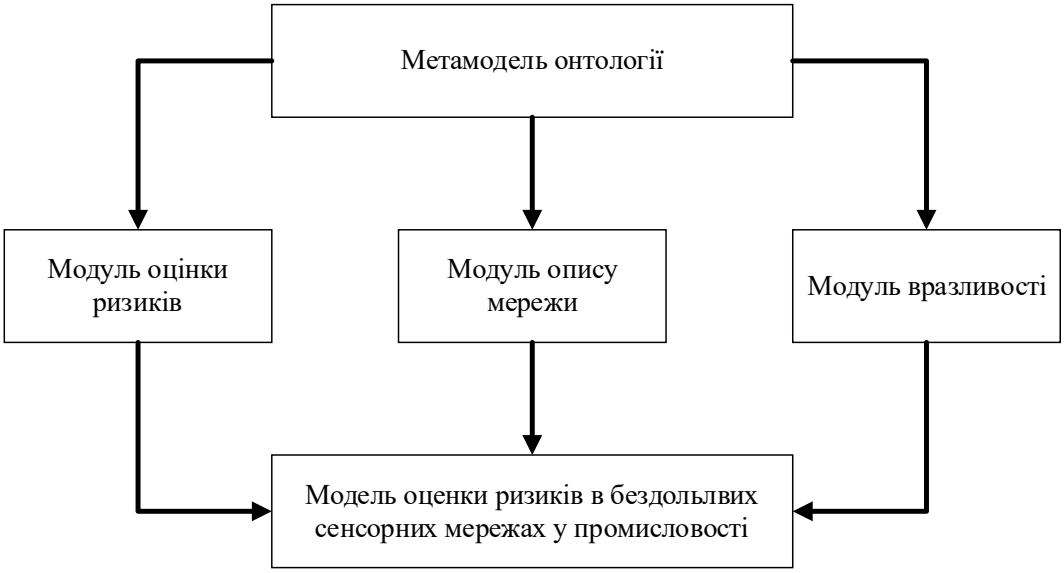

Рис. 1. **Багаторівнева модель онтології оцінки ризиків у БСМ у промисловості**

Ця схема є структурою метамоделі онтології, котра зв'язана із оцінкою ризиків у БСМ для промисловості. Схема використовує наступні ключові модулі:

1) модуль оцінки ризиків – виконує оцінку ризиків, які зв'язані із функціонуванням мережи;

2) модуль опису мережи – описує головні параметри та структуру БСМ;

3) модуль вразливості – виявляє вразливості у системі.

4) модуль оцінки ризиків у БСМ – є основним модулем та створює взаємодією між усіма трьома попередніми модулями.

Модуль вразливості є логічною системою, яка виконує аналіз структури БСМ та виявляє потенційні вразливості. Цей модуль відіграє ключову роль у оцінці ризиків, так як дозволяє визначити потенційно слабкі місця, котрі можуть бути використані задля нанесення шкоди системі. В основі підходу лежить побудова логічної моделі, яка описує різні елементи мережі та їх взаємозв'язки й відношення, а також можливі сценарії загроз.

Модуль вразливості складається за наступних компонентів:

– пристрої мережи – сенсори, актуатори, контролер, шлюзи, джерело живлення, а також параметри усіх пристроїв;

– з'єднання – протоколи передачі даних та їх властивості безпеки;

– зовнішні фактори - фізичний доступ, радіо інтерференція, атаки на протоколи;

– загрози – типи атак на мережу (перехоплення даних, вторгнення, втрата зв'язку, підміна вузлів).

Ця модель дозволяє формалізувати вразливості як об'єкти, їх зв'язки та відношення зі своїми атрибутами (тип загрози, ймовірність реалізації та потенційна шкода).

Система вразливості може бути представлена як набір логічних правил, котрі дозволяють виконати оцінку стану елементів мережи:

- Правило для виявлення вразливості у протоколі зв'язку – призначено для виявлення використання шифрування даних у протоколі зв'язку;
- правило для виявлення фізичних вразливостей – дана правило дозволяє виявити вразливість через некоректну роботу вузла, на яку впливають фізичні властивості зони покриття.

Модуль вразливості передає результати аналізу до модулю оцінки ризиків у БСМ. Логічні правила дозволяють модулю оцінювати сукупні ризики. Логічна система може постійно монітори мережи та виявляти нові вразливості на основі параметрів мережи та умов застосування. На основі логічного виводу модуль може автоматично пропонувати засоби

усунення вразливості.

У рамках розробки модуля вразливості бездротових сенсорних мереж для промислових застосувань пропонується використовувати математичну модель, яка враховує різні категорії загроз і їхній вплив на систему. Формула, що описує вразливість системи, може бути представлена наступним чином:

$$V = \alpha \times \sum_{i=1}^{n} P_i \times I_i + \beta \times \sum_{j=1}^{m} F_j \times S_j + \gamma \times \sum_{k=1}^{l} E_k \times T_k$$

де P_i, I_i – ймовірність та вплив технічних факторів;

F_j, S_j – фізичні фактори та їхній потенційний збиток;

E_k, T_k – зовнішні загрози та наслідки від їх реалізації;

α, β, γ – вагові коефіцієнти, що відображають важливість кожної категорії загроз у загальній системі оцінки ризиків.

Ця формула дозволяє моделювати сукупну вразливість мережі з урахуванням трьох ключових груп ризиків: технічних, фізичних і зовнішніх загроз. Вагові коефіцієнти можуть бути налаштовані залежно від конкретних умов експлуатації та особливостей мережі, забезпечуючи адаптацію моделі до різних промислових середовищ.

Застосування запропонованої моделі для конкретної мережі, що складається з 50 сенсорних вузлів, показує, що при оцінці вразливостей, таких як недостатнє шифрування даних або фізичний доступ до вузлів, кількість змінних значно зростає. Наприклад, у випадку використання декількох різних протоколів передачі даних та наявності кількох типів зовнішніх загроз (радіо інтерференція, фізичне втручання), складність обчислень збільшується через необхідність оцінювати кожен з цих факторів окремо. В реальних умовах, наприклад, в промисловому середовищі, де мережі функціонують у складних фізичних умовах, використання оптимізованих алгоритмів дозволяє виконувати моніторинг і оцінку ризиків в режимі реального часу, зводячи час реакції на потенційні загрози до мінімуму. Це забезпечує безперервну роботу системи навіть при високих вимогах до безпеки та надійності..

Висновки. У результаті дослідження було створено модуль вразливості для багаторівневої онтології оцінки ризиків у БСМ, що дозволяє виявляти слабкі місця мережі та оцінювати ризики за допомогою логічних правил. Модуль підвищує надійність і безпеку мережі завдяки постійному моніторингу в режимі реального часу. Прикладна логічна теорія забезпечує більше можливостей для опису предметної області порівняно з OWL. У подальшій роботі необхідно детальніше вивчити ефективність модуля в різних промислових умовах, оцінити його стійкість до різноманітних загроз та оптимізувати використання ресурсів мережі.

СПИСОК ЛІТЕРАТУРИ

1. Копитчук М. Б., Тішин П. М., Цюрупа М. В. «Аналіз вичислювальних мережей з допомоги багаторівньової онтології оцінки ризиків з застосуванням методології coras». *Електротехнічні та комп'ютерні системи*, 2013.

2. Paavola M., Leivisk K. “Wireless Sensor Networks in Industrial Automation”. *Factory Automation*. 2010. DOI: https://doi.org./10.5772/9532.

3. Wu H., Cao J., Fan X. “Dynamic collaborative event detection in wireless sensor networks, telecommun”. *Telecommunication Systems*. 2016; 62 (1): 43–58. DOI: https://doi.org./10.1007/ s11235-015-9981-0.

4. Karl H., Willing A. “Protocols and architectures for wireless sensor networks”. *John Wiley&Sons, Ltd*. 2005.

5. Znaidi W., Minier M., Babau, J.-P. “An Ontology for Attacks in Wireless Sensor Networks”. 2008.

6. Dharani, N., Krishnan K. , Mohan, K. “Wireless Sensor Network for Industrial Monitoring and Controlling”. *2021 5th International Conference on Intelligent Computing and Control Systems*. Madurai, India. 2021. p. 254-257. DOI: https://doi.org./10.1109/ICICCS51141. 2021.9432238.

7. Luis J., Gómez-Galán J. A., Bravo F., Sánchez-Raya M., Alcina-Espigado J., Teixido-Rovira, P. “An Efficient Wireless Sensor Network for Industrial Monitoring and Control”. *Sensors*. 2018; 18 (1): 182. DOI: https://doi.org./10.3390/s18010182.

8. Bendadouche R., Roussey C., Sousa G., Chane, J.-P., Hou K. “Extension of the Semantic Sensor Network Ontology for Wireless Sensor Networks: The Stimulus-WSNnode-Communication Pattern”. *5th International Workshop on Semantic Sensor Networks in conjunction with the 11th International Semantic Web Conference*. 2012.

9. Gholap B., Deore M. “Review of Condition Monitoring in the Railway Industry using Wireless Sensor Networks”. *6th International Conference on Internet of Things, Next Generation Networks and Cloud Computing*. 2021.

10. Duobienė S., Simniskis R., Raciukaitis G. “Enabling Seamless Connectivity: Networking Innovations in Wireless Sensor Networks for Industrial Application”. *Sensors*. 2024; 24 (15): 4881. DOI: https://doi.org./10.3390/s24154881.

11. Kim D.-Y., Cha S.-H., Cho K. H. “Ontology-Based Methodology for Managing Heterogeneous Wireless Sensor Networks”. *International Journal of Distributed Sensor Networks*. 2013; 13. DOI: https://doi.org./10.1155/2013/610684.

DOI: https://doi.org/10.15276/ict.01.2024.13
UDC 004.75

Vulnerability module in the multi-level ontology of risk assessment of Wireless Sensor Networks

Pavlo R. Shtilman[1)]
PhD student, Department of Computer Intellectual Systems and Networks Department
ORCID: https://orcid.org/0009-0007-8061-1766; pavel52shtilman62@gmail.com
Petr M. Tishin[1)]
PhD, Associated Professor, Department of Computer Intellectual Systems and Networks Department
ORCID: https://orcid.org/0000-0003-2506-5348; petrmettal@gmail.com. Scopus Author ID: 57190400970
[1)] Odesa Polytechnic National University, 1, Shevchenko Ave. Odesa, 65044, Ukraine

ABSTRACT

This work presents the development of a vulnerability module within a multi-level ontology for risk assessment in wireless sensor networks (WSNs) used in industrial environments. WSNs consist of multiple sensor nodes with microcontrollers, sensors, communication devices, and power sources, playing a key role in monitoring, diagnostics, and managing industrial processes. Their main advantages include reduced costs due to the lack of cabling and ease of scaling by adding new nodes. However, WSNs face significant challenges, including limited power supply, vulnerability to electromagnetic interference, low bandwidth, and exposure to cyber-attacks. These issues make them less suitable for real-time systems where fast and reliable data transmission is critical. The vulnerability module developed in this study addresses these challenges by identifying weaknesses, analyzing potential threats, and assessing risks using logical rules. These rules assess various network components such as devices, communication protocols, and external factors like physical access and radio interference. The module continuously monitors the network, detects new vulnerabilities, and provides real-time feedback to the risk assessment module, suggesting measures to mitigate risks. This enhances the security and reliability of WSNs in industrial applications. In conclusion, the vulnerability module within the multi-level ontology provides a structured approach to identifying and mitigating risks in WSNs. Despite the inherent vulnerabilities of WSNs, advancements in security protocols and energy efficiency make them increasingly viable for industrial automation and optimization.

Keywords: Wireless sensor networks (WSNs); vulnerabilities; risk assessment; industrial systems; logical rules; network security; cyber threats; energy efficiency; vulnerability module; network protocols; industrial automation; information security threats; ontology; Web Ontology Language (OWL)