КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (25), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.25.390400
УДК 004.6

Довженко Надія Михайлівна
кандидат технічних наук, доцент,
доцент кафедри інформаційної та кібернетичної
безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
доцент кафедри цифрових технологій в енергетиці
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна
ORCID ID: 0000-0003-4164-0066
nadezhdadovzhenko@gmail.com

Іваніченко Євген Вікторович
кандидат технічних наук, доцент,
заступник декана з науково-методичної та навчальної роботи
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0002-6408-443X
y.ivanichenko@kubg.edu.ua

Складанний Павло Миколайович
Кандидат технічних наук, доцент, завідувач кафедри
інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

Аушева Наталія Миколаївна
доктор технічних наук, професор,
завідувачка кафедри кафедри цифрових технологій в енергетиці
Національний технічний університет України «Київський
політехнічний інститут імені Ігоря Сікорського», Київ, Україна
ORCID ID: 0000-0003-0816-2971
nataauscheva@gmail.com

ІНТЕГРАЦІЯ БЕЗПЕКИ ТА ВІДМОВОСТІЙКОСТІ СЕНСОРНИХ МЕРЕЖ НА ОСНОВІ АНАЛІЗУ ЕНЕРГОСПОЖИВАННЯ ТА ТРАФІКУ

Анотація. У статті досліджено особливості функціонування сенсорних мереж як ключової складової технології Інтернету речей (IoT), що забезпечує інтеграцію між фізичним і цифровим світом. Проаналізовано виклики, з якими стикаються сенсорні мережі, включаючи обмежені ресурси, збої вузлів, масштабування та загрози безпеці. Розглянуто основні компоненти сенсорних мереж: датчики, сенсори, «інтелектуальні» елементи, шлюзи та комунікаційні модулі, які забезпечують збір і передачу даних для подальшого аналізу. Акцентовано увагу на тому, що сенсорні мережі часто є мішенню для атак зловмисників, таких як DDoS, Sinkhole і атаки на маршрутизацію, що вимагає розробки нових методів захисту. Детально розглянуто загрози від нелегітимних елементів у сенсорних мережах, які можуть порушувати роботу мережі, створювати витоки даних та впливати на живучість і відмовостійкість мережі шляхом виснаження ресурсів. Для ефективного виявлення таких вузлів запропоновано застосовувати механізми аналізу та моніторингу трафіку, енергоспоживання та шифрування. Досліджено природу збоїв у сенсорних мережах та взаємозв'язок відмовостійкості й безпеки. Розраховано ймовірності відмов для мереж різних розмірів та запропоновано механізми підвищення відмовостійкості, включаючи резервування вузлів, алгоритми самовідновлення та толерантність до помилок. Запропоновано методику виявлення зловмисних вузлів на основі аналізу трафіку та

© Н.М. Довженко, Є.В. Іваніченко, П.М. Складанний, Н.М. Аушева, 2024

енергетичних характеристик. Виявлено, що вузли, які перевищують порогові значення за кількістю переданих пакетів або енергоспоживанням, можуть бути зловмисними. Зазначено, що комбінування різних методів дозволить підвищити точність виявлення зловмисних вузлів на ранніх етапах, що значно покращить рівень інформаційної безпеки сенсорних мереж. Висвітлено перспективи подальших досліджень у напрямку розробки нових захисних механізмів та підвищення відмовостійкості сенсорних мереж.

Ключові слова: Інтернет Речей; IoT; інформаційна безпека; сенсорна мережа; енергоресурси; відмовостійкість; загрози; аномалії; надійність; вузли.

ВСТУП

Сьогодні значна кількість пристроїв та систем у світі підключена до мережі Інтернет. Постійно відбувається взаємодія між користувачами, пристроями та обладнанням. Технічна та автоматизована взаємодія призводить до появи нових застосунків, послуг та технологій, які здатні певним чином покращувати життя людей.

Технологія Інтернету речей (IoT) часто розглядається як суттєвий технологічний прорив, який змінив підхід до взаємодії між фізичними та цифровими системами. Здавалося б, прості елементи набули здатності сприймати, «зчитувати», первинно опрацьовувати та контролювати фізичний світ, надаючи їм «інтелектуальні» можливості та об'єднуючи їх у єдині, спеціалізовані мережі IoT [1].

Завдяки можливостям дистанційного моніторингу та управління постійно відбувається інтеграція між фізичним світом та цифровими системами через використання сенсорів, датчиків, актуаторів та технологій обробки даних [2]. Це сприяє підвищенню ефективності, точності, автоматизації та безпеки процесів, що є основою для створення нових та вдосконалення наявних IoT-застосунків.

Світ Інтернету речей (IoT) є широким і багатогранним, охоплює різноманітні галузі, кожна з яких має свої особливості та технологічні вимоги. Однак доцільніше розглядати його не як єдиний технологічний домен, а як сукупність різних концепцій, протоколів і технологій, що змінюються залежно від галузі застосування [3].

Сенсорні мережі є ключовою частиною IoT, забезпечуючи моніторинг фізичних параметрів навколишнього середовища. Однак через обмежені ресурси та роботу в суворих умовах ці мережі часто стикаються з проблемами несправностей вузлів і відмов, що призводить до нових викликів, зокрема масштабування мережі для великої кількості підключених пристроїв, обробки значних обсягів даних і, звичайно, безпеки [4].

АКТУАЛЬНІ ВИКЛИКИ В СЕНСОРНИХ МЕРЕЖАХ

До основних компонентів сенсорних мереж можна віднести сенсори, датчики, комунікаційні модулі, шлюзи та центри обробки даних. Перелік не є вичерпним, і додавання нових елементів до мережі може бути легко обґрунтоване необхідністю, фізичним або мережевим ландшафтом та вимогами масштабованості мережі для підтримки більшої кількості підключених пристроїв.

Сенсорні мережі складаються з сотень й тисяч вузлів, що збирають дані, первинно обробляють та передають їх до центральних серверів або хмарних платформ з використанням безпроводових протоколів передачі інформації для подальшого аналізу. Хоча більшість даних, створених в сенсорних мережах, є неструктурованими, розуміння,

яке вони надають за допомогою аналітики, може революціонізувати процеси та створити нові бізнес-моделі [5].

Загалом, більшість IT-організацій не надто переймаються неструктурованими даними, що генеруються подібними елементами в мережі. Однак в IoT дані, отримані від сенсорних датчиків, це цінним ресурсом. Вони дозволяють компаніям надавати нові, актуальні послуги, які однозначно покращують взаємодію з клієнтами, знижують витрати та створюють нові можливості для отримання прибутку.

Основними проблемами, з якими стикаються сенсорні мережі, є обмеженість енергетичних ресурсів, збої та відмови в роботі сенсорів та вузлів, атаки зловмисників, такі як DDoS, перехоплення даних, Sinkhole атака та атаки на маршрутизацію, та інші технічні несправності [6].

ДОСЛІДЖЕННЯ ЗАГРОЗ ВІД НЕЛЕГІТИМНИХ ЕЛЕМЕНТІВ У СЕНСОРНИХ МЕРЕЖАХ

Поява нелегітимних елементів в сенсорних мережах поширена практика серед зловмисників. Такі дії становлять суттєву загрозу, наприклад, для корпоративних мереж, частина з яких може бути реалізована в беспроводовому середовищі із сотень датчиків та сенсорів [7].

Такий вузол може бути доданий до мережі для конкретних зловмисних цілей: порушення коректної роботи мережі або окремих її сегментів, створення витоків конфіденційних даних, імплементування шкідливого програмного забезпечення, вплив на живучість та відмовостійкість мережі шляхом виснаження внутрішніх ресурсів чи порушення зв’язності між вузлами тощо.

На рис. 1. наведено приклад алгоритму дій зловмисного, нелегітимного вузла в СМ.

Зловмисник може отримати доступ до мережі кількома способами: фізичне підключення, шляхом підміни одного із елементів мережі або використовуючи вразливості в процесі автентифікації та авторизації (фактично вразливості в процесах отримання доступу). Після успішності цього кроку, нелегітимний вузол може спробувати встановити з’єднання з іншими вузлами. На цьому кроці можуть бути використанні протоколи для обміну даними, підроблені ідентифікатори. Ціль зловмисника — створити враження, що вузол є легітимним елементом мережі.

Паралельно можуть виконуватися й інші атаки, такі як jamming, перехоплення або модифікація даних, атаки типу «людина посередині», підрив енергоресурсів тощо.

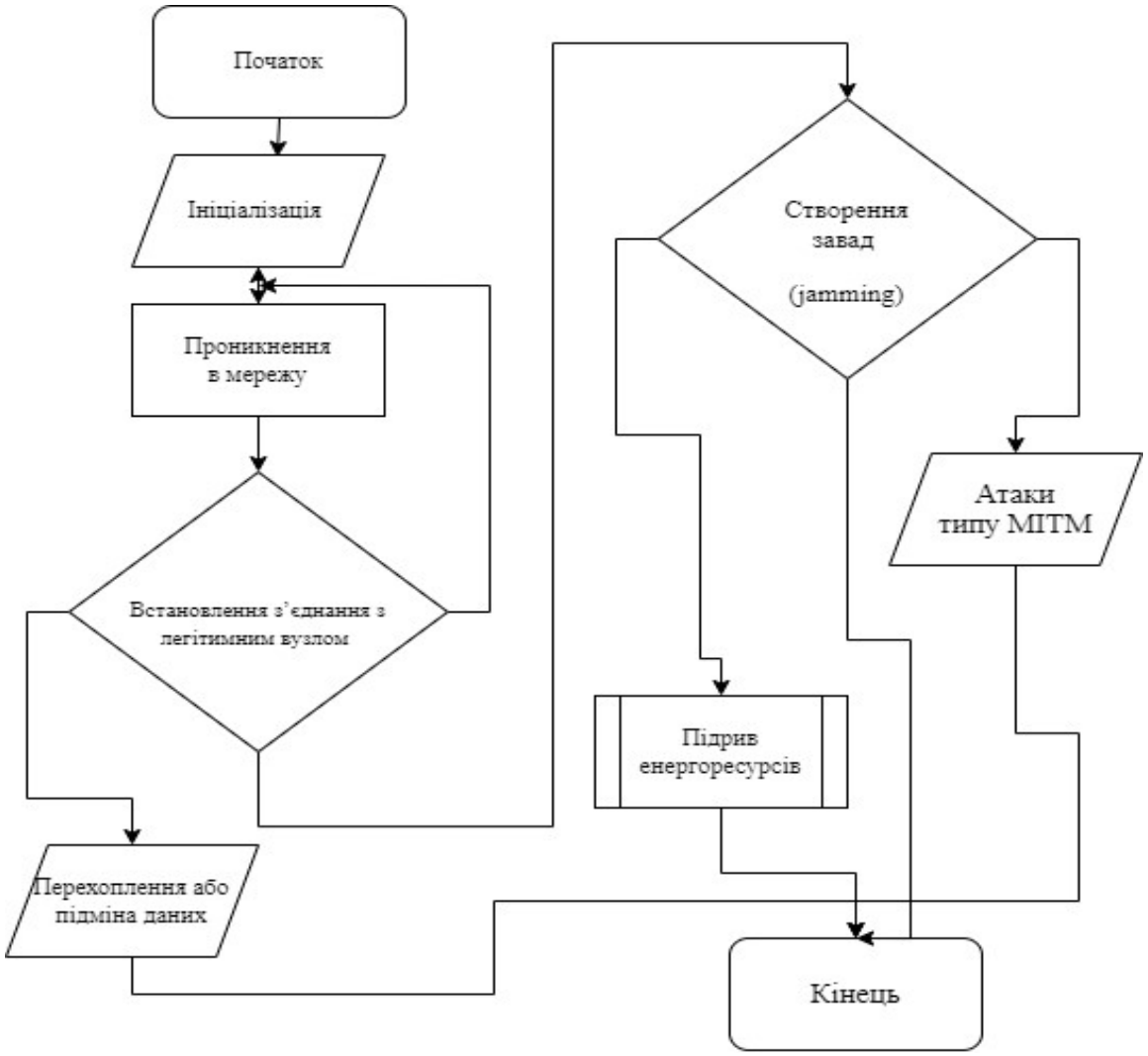

Рис. 1. Алгоритм дій зловмисного вузла в сенсорній мережі

Нелегітимний сенсорний вузол здатен суттєво вплинути на роботу мережі через створення завад, маніпуляцію даними та витрату ресурсів. Для виявлення подібної поведінки та ефективній протидії таким загрозам необхідно використовувати комбінування дій: застосування механізмів автентифікації, шифрування, відстежування мережевого трафіку, моніторинг та виявлення аномалій для забезпечення надійної безпеки сенсорних мереж як компонентів IoT [8].

РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ

Дослідження природи збоїв демонструє, що відмовостійкість та безпека в сенсорних мережах тісно взаємопов'язані між собою та формують узагальнену структуру надійної системи, яка здатна протидіяти як внутрішнім збоям та відмовам, так і зовнішнім загрозам, деструктивному впливу зловмисників [9].

Для прикладу взаємозв'язку відмовостійкості та безпеки можна розглянути сенсорну мережу, яка складається з 50, 100, 200 та 500 вузлів. Якщо елементи мережі функціонують автономно, ймовірність того, що всі вузли в мережі працюють без відмов та збоїв буде розраховуватися наступним чином: $(1-p)^n$.

Можна припустити, що ймовірність відмови кожного окремого вузла протягом певного періоду становитиме 0.01 (тобто 1%). Ймовірність того, що жоден вузол не відмовить, можна розрахувати за формулою:

$$P = (1 - p)^n, \quad (1)$$

де n — це кількість вузлів у сенсорної мережі.

Для мережі, що складається з 50 вузлів ймовірність безвідмовної роботи всіх елементів становить приблизно 60,5%; для мережі зі 100 вузлів ця ймовірність знижується до 36,6%; для 200 вузлів — 13,4%, а для 500 вузлів ймовірність становить лише 0,66%.

На рис. 2. продемонстровано, що зі збільшенням кількості вузлів зростає й загальна ймовірність відмови всієї мережі. Це підкреслює важливість впровадження механізмів для підвищення відмовостійкості, таких як резервування вузлів, самовідновлення або алгоритми толерантності до помилок тощо [10], особливо в умовах проєктування мереж зі значно більшою кількістю сенсорних вузлів.

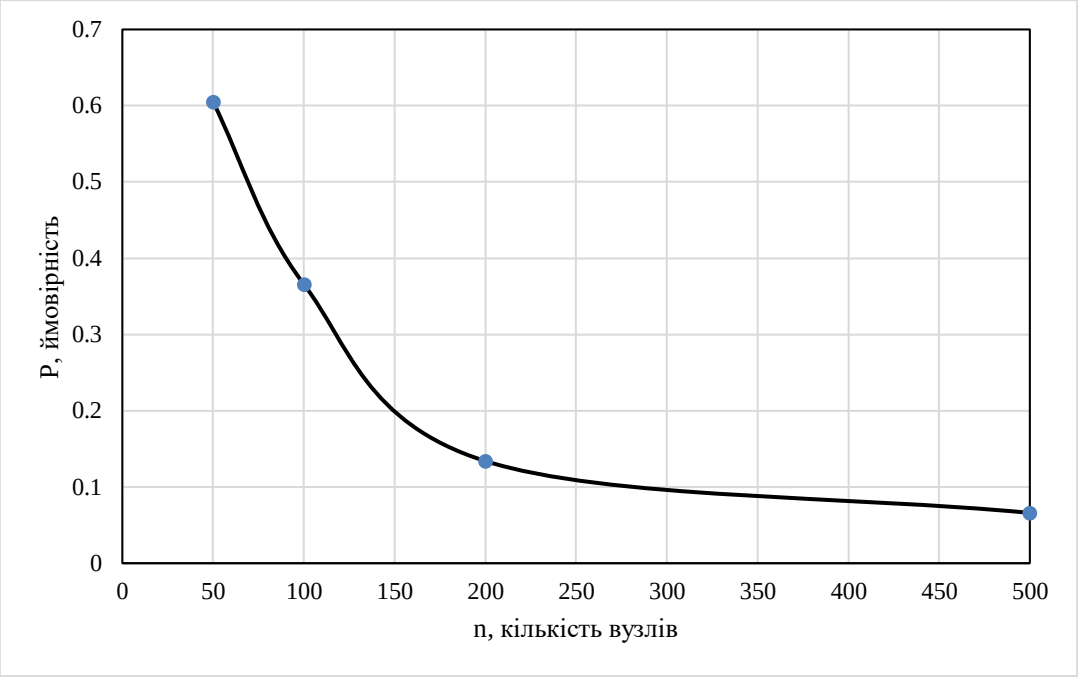

Рис. 2. Вплив зміни кількості вузлів на ймовірність відмови сенсорної мережі

Виявлення нелегітимного сенсорного вузла може бути здійснено через декілька методів аналізу поведінки вузлів у мережі.

Методика виявлення нелегітимних вузлів у сенсорних мережах за допомогою аналізу трафіку та порогових значень. Для виявлення появи нелегітимного сенсорного вузла в мережі можна виконати декілька кроків, а саме здійснити розрахунки аналізу поведінки вузлів у мережі. Більшість науковців звертаються до використання статистичних або евристичних методів, які аналізують трафік та поведінку кожного вузла на основі певних параметрів.

За основу можна взяти спрощений підхід до виявлення нелегітимного вузла за допомогою аналізу аномальної активності та енергетичних характеристик.

Наприклад, проєктується сенсорна мережа із загальною кількістю елементів, що дорівнюють значенню N, $N = 100$ вузлів. При цьому, середня кількість пакетів,які

ISSN 2663 - 4023

передаються вузлом в мережі за певний проміжок часу, можна визначити як P_{leg} (наприклад, 50 пакетів за хвилину).

Порогові значення (максимально допустима кількість пакетів для вузла, що вважається легітимним) також доцільно розраховувати та визначати для кожної проєктованої мережі. Цей параметр визначається як P_{max}, та може умовно складати 60 пакетів за хвилину. Це дасть змогу врахувати незначні відхилення. Кількість пакетів, переданих нелегітимним вузлом, визначається як параметр P_k.

Якщо вузол передає певну кількість пакетів, яка перевищує значення P_{max}, то мережа може визнати його як нелегітимний або ж зловмисний. Тому можуть бути прийняті певні кроки, щоб діагностувати аномалію та визначити несправності в роботі такого елемента в мережі.

Для цього проводиться моніторинг трафіку, під час якого вимірюється кількість пакетів, переданих кожним вузлом за певний період часу, наприклад, за одну хвилину. Окремо враховується середнє значення для всіх елементів в мережі:

$$P_{aver} = \frac{1}{N}\sum_{i=1}^{N} P_i, \qquad (2)$$

де P_i — кількість пакетів, які передав i — вузол сенсорної мережі. Було припущено, що $P_{aver} = 50$ пакетів.

Для визначення значення появи в мережі нелегітимного вузла використовують фіксоване, порогове значення. Наприклад, якщо для будь-якого вузла сенсорної мережі виконуватиметься значення $P_i > P_{max}$, де $P_{max} = P_{aver} + 10$, то такий вузол буде визначено як зловмисний або потенційно нелегітимний[11].

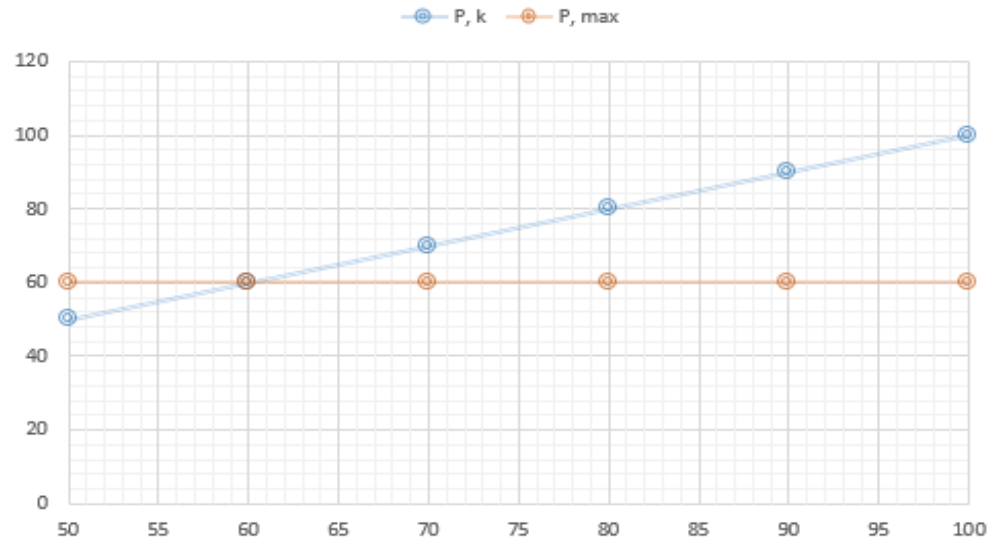

Рис. 3. Виявлення нелегітимних вузлів на основі аналізу трафіку

На рис. 3 відображено залежність кількості пакетів, переданих вузлами сенсорної мережі P_k і порогового значення P_{max}, яке визначає, чи є вузол легітимним або зловмисним.

Якщо один із вузлів в певний проміжок часу передає понад 50 пакетів умовно за хвилину, і це значення варіюється в діапазоні понад 100 пакетів, тобто, якщо $P_k > P_{max}$, то такий вузол також визначається як зловмисний.

ISSN 2663 - 4023

Методика виявлення нелегітимних вузлів у сенсорних мережах за допомогою аналізу енергетичних втрат. Так як сенсорні мережі складаються із значної кількості безпроводових інтелектуальних об'єктів, існує цілий ряд обмежень, які слід враховувати при проєктуванні. До найважливіших показників можна віднести: обмеження потужності обробки запитів, втрати підключень, обмеження пам'яті, обмеження щодо швидкості передачі та обмеження потужності. Перераховані обмеження значною мірою впливають на те, як розробляються, розгортаються та використовуються сенсорні мережі [12].

Нелегітимний вузол може виділятися при функціонуванні розгорнутої СМ через аномальну активність, споживаючи значно більше енергоресурсів ніж сусідні елементи. Виникнути може така ситуація через часті передачі трафіку зловмиснику. Припустимо, що спочатку необхідно розрахувати значення енергії, яку споживає кожен вузол під час передачі пакетів за певний час. Далі необхідно здійснити порівняння. Якщо значення для вузла суттєво перевищує середній показник, його діяльність може визначатися як підозріла:

$$E_k > E_{aver} * 1{,}5, \quad (3)$$

де E_k — енергетичні витрати нелегітимного вузла, який надсилає більше пакетів (може перевищувати середній показник), E_{aver} — середнє споживання енергії для вузлів у мережі, а 1,5 — коефіцієнт, який може варіюватися залежно від особливостей сенсорної мережі [13].

Нелегітимний вузол може споживати більше енергії через безперервну активність (наприклад jamming, перехоплення або модифікація даних, атаки типу «людина посередині», підрив енергоресурсів тощо)і це значення може бути розраховане:

$$E_k = 2 * E_{leg} \quad (4)$$

де E_{leg} — середні енергетичні витрати легітимного вузла на передачу одного пакету (наприклад, 0.01 Дж), 2 — коефіцієнт отриманий на основі спостережень, при яких зловмисні вузли втрачають в 2 рази більше енергоресурсів через залучення до атак та через постійні передачі даних [14].

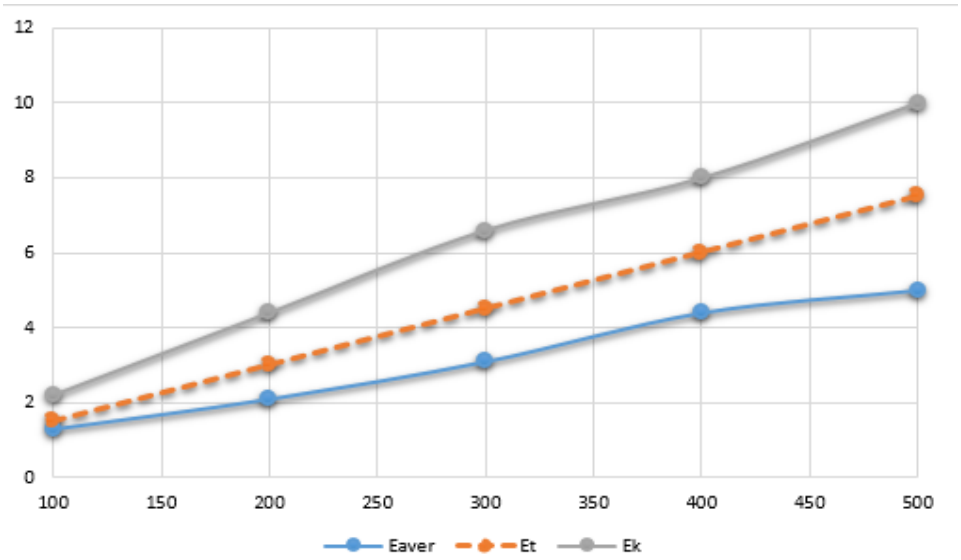

Рис. 4. Аналіз енергетичних витрат у СМ

Значення E_{aver} представляє середні енергетичні витрати легітимних вузлів, тоді як E_k — демонструє енергетичні витрати зловмисного вузла, які перевищують середні витрати звичанйих елементів мережі. Порогове значення E_t визначається як значення, що перевищує середні показники E_{aver} на 1,5 рази.

Результати розрахунків, приведені на рис. 2–4 показують, що зловмисні вузли споживають значно більше ресурсів, перевищуючи порогові значення в 1,5–2 рази.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

З розвитком IoT-технологій з'являються нові виклики, зокрема у сфері кібербезпеки. Необхідно розробляти нові методи захисту від сучасних та майбутніх загроз, таких як квантові атаки, що можуть обійти традиційні криптографічні методи.

В процесі дослідження було встановлено, що для виявлення появи в мережі нелегітимного або зловмисного сенсорного вузла можна використовувати кілька методів, наприклад аналіз кількості переданих пакетів та аналіз енергоспоживання. В першому випадку, якщо кількість пакетів перевищує певні порогові значення, це може свідчити про початок атаки та про зловмисну діяльність. В другому випадку, нелегітимний вузол споживатиме більше енергії через постійну активність і необхідність частішої активації та передачі трафіку.

Варто підкреслити, що для покращення точності виявлення зловмисних вузлів та відслідковування їх аномальної поведінки доцільно використовувати комбінування різних методів, що дасть змогу виявляти загрози на ранніх етапах, підвищуючи рівень інформаційної безпеки в сенсорній мережі.

В майбутньому доцільно зосередити увагу та зусилля науковців на розробці нових та покращення наявних механізмів, які знижують вплив зловмисних елементів в мережах, мінімізують втрати ресурсів легітимних вузлів і підвищують їх живучість та відмовостійкість.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Comput. Netw. 76,* 146–164. https://doi.org/10.1016/j.comnet.2014.11.008
2. Барабаш, О. В., Довженко, Н. М., & Аушева, Н. М. (2024). Інтегрований підхід до забезпечення безпеки в сенсорних мережах. *XI Всеукраїнська науково–практична конференція молодих учених,* 223–224.
3. Liu, D., & Ning, P. (2007). Security for Wireless Sensor Networks. *Advances in Information Security (ADIS), 28*. https://doi.org/10.1007/978-0-387-46781-8
4. Zhang, H., Liu, J., & Kato, N. (2018). Threshold Tuning-Based Wearable Sensor Fault Detection for Reliable Medical Monitoring Using Bayesian Network Model. *IEEE Syst. J. 12,* 1886–1896. https://doi.org/10.1109/JSYST.2016.2600582
5. Openko, P., Dovzhenko, N., Orikhovsky, P., & Ikaev, D. (2024). Ensuring reliability and security in modern wireless sensor networks based on the implementation of the RSSI metric. *Air power of Ukraine, 1(6),* 131–136. https://doi.org/10.33099/2786-7714-2024-1-6-131-136
6. Dovzhenko, N., Barabash, O., Ausheva, A., Ivanichenko, Y., & Obushnyi S. (2023). Comprehensive Analysis of Efficiency and Security Challenges in Sensor Network Routing. In *Cybersecurity Providing in Information and Telecommunication Systems, CPITS-II 2023, vol. 3550,* 275–280.
7. Zawaideh, F. (2019). An Efficient Weighted Trust-Based Malicious Node Detection Scheme for Wireless Sensor Networks. *Int. J. Commun. Syst. 32,* 3878. https://doi.org/10.1002/dac.3878

8. John, A., Isnin, F. I., & Madni, S. H. H. (2023). Current security threats in applications of wireless sensor network. *International Journal of Engineering, Science and Technology (IJonET), 5(3),* 255–272. https://doi.org/10.46328/ijonest.174
9. Ahmad, R, Wazirali, R, & Abu-Ain, T. (2022). Machine Learning for Wireless Sensor Networks Security: An Overview of Challenges and Issues. *Sensors, 22(13),* 4730. https://doi.org/10.3390/s22134730
10. Barabash, O., Ausheva, N., Skladannyi, P., Ivanichenko, Y., & Dovzhenko, N. (2024). Technical aspects of building a fault-tolerant sensor network infrastructure. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique», 4(24),* 185–195. https://doi.org/10.28925/2663-4023.2024.24.185195
11. Kim, T., Vecchietti, L. F., Choi, K., Lee, S., & Har, D. (2021). Machine Learning for Advanced Wireless Sensor Networks: A Review. *IEEE Sens. J. 21,* 12379–12397. https://doi.org/10.1109/JSEN.2020.3035846
12. Karpenko, A., Bondarenko, T., Ovsiannikov, V., & Martyniuk, V. (2020). Ensuring information security in wireless sensor networks. *Electronic professional scientific publication "Cybersecurity: Education, Science, Technology", 2(10),* 54–66. https://doi.org/10.28925/2663-4023.2020.10.5466
13. Jain, U., & Hussain, M. (2018). Wireless Sensor Networks: Attacks and Countermeasures. *SSRN Electronic Journal.* https://doi.org/10.2139/ssrn.3170185
14. Karlof, C., & Wagner D. (2003). Secure routing in wireless sensor networks: attacks and countermeasures. *Ad Hoc Networks. 1(2–3),* 293–315. https://doi.org/10.1016/s1570-8705(03)00008-8

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (25), 2024
ISSN 2663 - 4023

Nadiia Dovzhenko
PhD, Associate Professor, Associate Professor of the Department of
Information and Cybernetic Security named after Professor Volodymyr Buryachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
Associate Professor of the Department of Digital Technologies in Energy
National Technical University of Ukraine «Igor Sikorsky Kyiv
Polytechnic Institute», Kyiv, Ukraine
ORCID ID: 0000-0003-4164-0066
nadezhdadovzhenko@gmail.com

Yevhen Ivanichenko
PhD, Associate Professor,
Deputy Dean for Scientific-Methodological and Educational Work
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0002-6408-443X
y.ivanichenko@kubg.edu.ua

Pavlo Skladannyi
PhD, Associate Professor, Head of the Department of
Information and Cyber Security named after Professor Volodymyr Buryachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

Nataliya Ausheva
Doctor of Technical Sciences, Professor,
Head of the Department of Digital Technologies in Energy
National Technical University of Ukraine «Igor Sikorsky Kyiv
Polytechnic Institute», Kyiv, Ukraine
ORCID ID: 0000-0003-0816-2971
nataauscheva@gmail.com

INTEGRATION OF SECURITY AND FAULT TOLERANCE IN SENSOR NETWORKS BASED ON THE ANALYSIS OF ENERGY CONSUMPTION AND TRAFFIC

Abstract. This article examines the functioning of sensor networks as a key component of the Internet of Things (IoT) technology, which facilitates integration between the physical and digital worlds. It analyzes the challenges sensor networks face, including limited resources, node failures, scalability, and security threats. The main components of sensor networks are discussed: sensors, smart elements, gateways, and communication modules that enable data collection and transmission for further analysis. Attention is drawn to the fact that sensor networks are often targets of malicious attacks, such as DDoS, Sinkhole, and routing attacks, which necessitate the development of new protection methods. The paper thoroughly examines threats from illegitimate elements in sensor networks that can disrupt network operations, cause data leaks, and affect network resilience and fault tolerance by exhausting resources. To effectively detect such nodes, it is proposed to apply mechanisms for traffic analysis, energy consumption monitoring, and encryption. The nature of failures in sensor networks and the interrelationship between fault tolerance and security are explored. Probabilities of failure for networks of different sizes are calculated, and mechanisms for improving fault tolerance, including node redundancy, self-healing algorithms, and fault tolerance mechanisms, are proposed. A methodology for detecting malicious nodes based on traffic and energy characteristics analysis is suggested. It was found that nodes exceeding threshold values for the number of transmitted packets or energy consumption may be malicious. It is noted that combining various methods will improve the accuracy of detecting malicious nodes at early stages, significantly enhancing the level of information security in sensor networks. Prospects for further research into the development of new protective mechanisms and improvements in the fault tolerance of sensor networks are highlighted.

Keywords: Internet of Things; IoT; information security; sensor network; energy resources; fault tolerance; threats; anomalies; reliability; nodes.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Comput. Netw. 76*, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008
2. Barabash, O. V., Dovzhenko, N. M., & Ausheva, N. M. (2024). An integrated approach to security in sensor networks. *XI All-Ukrainian scientific and practical conference of young scientists*, 223–224.
3. Liu, D., & Ning, P. (2007). Security for Wireless Sensor Networks. *Advances in Information Security (ADIS), 28*. https://doi.org/10.1007/978-0-387-46781-8
4. Zhang, H., Liu, J., & Kato, N. (2018). Threshold Tuning-Based Wearable Sensor Fault Detection for Reliable Medical Monitoring Using Bayesian Network Model. *IEEE Syst. J. 12*, 1886–1896. https://doi.org/10.1109/JSYST.2016.2600582
5. Openko, P., Dovzhenko, N., Orikhovsky, P., & Ikaev, D. (2024). Ensuring reliability and security in modern wireless sensor networks based on the implementation of the RSSI metric. *Air power of Ukraine, 1(6),* 131–136. https://doi.org/10.33099/2786-7714-2024-1-6-131-136
6. Dovzhenko, N., Barabash, O., Ausheva, A., Ivanichenko, Y., & Obushnyi S. (2023). Comprehensive Analysis of Efficiency and Security Challenges in Sensor Network Routing. In *Cybersecurity Providing in Information and Telecommunication Systems, CPITS-II 2023, vol. 3550,* 275–280.
7. Zawaideh, F. (2019). An Efficient Weighted Trust-Based Malicious Node Detection Scheme for Wireless Sensor Networks. *Int. J. Commun. Syst. 32,* 3878. https://doi.org/10.1002/dac.3878
8. John, A., Isnin, F. I., & Madni, S. H. H. (2023). Current security threats in applications of wireless sensor network. *International Journal of Engineering, Science and Technology (IJonET), 5(3),* 255–272. https://doi.org/10.46328/ijonest.174
9. Ahmad, R, Wazirali, R, & Abu-Ain, T. (2022). Machine Learning for Wireless Sensor Networks Security: An Overview of Challenges and Issues. *Sensors, 22(13),* 4730. https://doi.org/10.3390/s22134730
10. Barabash, O., Ausheva, N., Skladannyi, P., Ivanichenko, Y., & Dovzhenko, N. (2024). Technical aspects of building a fault-tolerant sensor network infrastructure. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique», 4(24),* 185–195. https://doi.org/10.28925/2663-4023.2024.24.185195
11. Kim, T., Vecchietti, L. F., Choi, K., Lee, S., & Har, D. (2021). Machine Learning for Advanced Wireless Sensor Networks: A Review. *IEEE Sens. J. 21*, 12379–12397. https://doi.org/10.1109/JSEN.2020.3035846
12. Karpenko, A., Bondarenko, T., Ovsiannikov, V., & Martyniuk, V. (2020). Ensuring information security in wireless sensor networks. *Electronic professional scientific publication "Cybersecurity: Education, Science, Technology", 2(10),* 54–66. https://doi.org/10.28925/2663-4023.2020.10.5466
13. Jain, U., & Hussain, M. (2018). Wireless Sensor Networks: Attacks and Countermeasures. *SSRN Electronic Journal.* https://doi.org/10.2139/ssrn.3170185
14. Karlof, C., & Wagner D. (2003). Secure routing in wireless sensor networks: attacks and countermeasures. *Ad Hoc Networks. 1(2–3),* 293–315. https://doi.org/10.1016/s1570-8705(03)00008-8

(cc) BY-NC-SA

This work is licensed under Creative Commons Attribution-noncommercial-sharealike 4.0 International License.