КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (24), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.24.185195
УДК 004.6

Барабаш Олег Володимирович
д.т.н., професор, професор кафедри
інженерії програмного забезпечення в енергетиці
Національний технічний університет України «Київський
політехнічний інститут імені Ігоря Сікорського», Київ, Україна
ORCID ID: 0000-0003-1715-0761
bar64@ukr.net

Аушева Наталія Миколаївна
д.т.н., професор, завідувачка 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

Складанний Павло Миколайович
к.т.н., 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

Іваніченко Євген Вікторович
к.т.н., 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

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

ТЕХНІЧНІ АСПЕКТИ ПОБУДОВИ ВІДМОВОСТІЙКОЇ ІНФРАСТРУКТУРИ СЕНСОРНОЇ МЕРЕЖІ

Анотація. У статті розглянуто особливості функціонування та сфери застосування сенсорних мереж, що включають моніторинг навколишнього середовища, військові застосування, управління «розумними» будівлями та «смарт» містами. Проаналізовано необхідність забезпечення відмовостійкості та енергоефективності елементів таких мереж. Зазначено, що сучасні сенсорні мережі здатні автономно реагувати на зміни в середовищі розгортання та експлуатації, підтримуючи робочий стан навіть за умов збоїв та перешкод. Досліджено різні методи забезпечення відмовостійкості, серед яких можна виділити використання алгоритмів самоконфігурації, ротацію ролей між датчиками, ієрархічні системи управління вузлами мережі тощо. Підкреслено необхідність створення нових та покращення чинних енергоефективних протоколів, які здатні мінімізувати споживання енергії як окремими вузлами, так і підвищити автономність та більш надійне та безвідмовне функціонування сегментів сенсорної мережі. Проаналізовано вплив зменшення та збільшення кількості вузлів на відмовостійкість мережі та їх здатність до самовідновлення в умовах аномального та зловмисного втручання. Зазначено необхідність вдосконалення механізмів захисту від подібних втручань для підвищення надійності та стійкості

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

мереж. Окремо підкреслено наслідки від зростаючого впливу новітніх загроз та вразливостей на безпеку сенсорних мереж, що вимагає постійного моніторингу, пошуку надійних та продуктивних рішень, оновлення та покращення захисних механізмів. Додатково проаналізовано адаптивні алгоритми управління ресурсами та трафіком, які здатні швидко реагувати на зміни умов експлуатації та запобігати аномаліям інформаційній безпеці. Зазначено, що досягнення високого рівня відмовостійкості та енергоефективності сенсорних мереж є ключовим фактором їх успішного використання в критичних застосуваннях. Проаналізовано перспективи подальших досліджень у галузі енергоефективності та відмовостійкості сенсорних мереж.

Ключові слова: сенсорна мережа; безпека; відмовостійкість; загрози; аномалії; надійність; вузли; БПЛА.

ВСТУП

Невпинне зростання вартості енергоресурсів, сировини та матеріалів, а також зростаючі вимоги до ефективності виробничих процесів сприяли розширення застосування сенсорних мереж у різних галузях. У відповідь на останні тенденції, сенсорні мережі, які об'єднують значну кількість «розумних» приладів, сенсорів та датчиків в єдину мережу, використовуються для неперервної взаємодії та обміну даними. Щодня ці мережі, які використовують сучасні досягнення в області безпроводових технологій, стають невіддільним інструментом у наданні оперативних та достовірних даних для широкого спектра застосувань, від екологічного моніторингу до управління «розумними» складовими та промислових процесів. Відтак постійно зростають все нові вимоги до забезпечення безпеки як окремих компонентів таких мереж, також і до їх безпечного та стійкого функціонування [1].

Сьогодні сенсорні мережі складаються із значної кількості вузлів, частіше за все децентралізованих та оснащених елементами енергоживлення, які здатні отримувати, опрацьовувати та ретранслювати зібрані дані. Інформація, зібрана цими вузлами, передається між іншими елементами мережі або надсилається на центральний шлюз (станцію) для подальшої обробки. Завдяки можливості ретрансляції сигналів від одного вузла до іншого, радіус дії такої мережі може коливатися від декількох метрів до кількох кілометрів [2].

Питання побудови сучасних конвергентних мереж, покращення безпеки та функціонування сенсорних мереж, їх відмовостійкості на надійності, досліджували в своїх працях Романюк В. А., Міночкін А. І., Яцків В. В., Якимчук Н. М, Жук А. В., Машков О. А., Субач І. Ю, Савченко В. А., Обідін Д. М., Akyildiz I., Ahlswede R. тощо.

ЗАБЕЗПЕЧЕННЯ ВІДМОВОСТІЙКОСТІ В СЕНСОРНИХ МЕРЕЖАХ

Звичайно що останнім часом елементи сенсорної мережі здатні автономно реагувати на зміни в середовищі, наприклад, підтримувати робочий стан у відповідь на зміну температури, регулювати освітлення у приміщенні або ж автоматично знаходити альтернативні маршрути у випадку відмови в роботі. Цю спроможність ефективно функціонувати навіть за умов збоїв, перешкод чи змін у зовнішніх умовах забезпечує відмовостійкість сенсорних мереж.

Особливо це набуває актуальності та відіграє значну роль в системах, які використовуються для моніторингу навколишнього середовища, у військових цілях, при управлінні «розумними» будівлями та «розумними» містами [3].

Забезпечення необхідного рівня стійкості дозволяє сенсорним мережам залишатися надійними та ефективними у критичних застосуваннях, підтримуючи їхню здатність до самовідновлення і адаптації в динамічних умовах.

Ефективне управління ресурсами та компонентами сенсорної мережі, а також їх безпекою, вимагає детального аналізу та вивчення сучасних тенденцій і загроз, що є важливим для забезпечення функціональної стійкості. Це вимагає комплексного підходу, який включає розробку новітніх механізмів захисту, управління трафіком, оптимізації споживання енергії та ефективного використання ресурсів тощо [4].

Вузли сенсорної мережі часто живляться від елементів електроживлення та при цьому повинні швидко адаптуватися до змін у середовищі. Оптимізація споживання енергії забезпечує довший термін служби вузлів та знижує частоту їх обслуговування. Однак часто виникають сценарії аномального використання сигналізації або смуги пропускання, які можуть призвести до неефективного використання енергії та мережевих ресурсів, наприклад:

- якщо режим очікування таймера мережі встановлено на десять секунд, встановлення сесії відбувається з додатковою допомогою сигналізації кожні 11 секунд. Це призводить до того, що за одну годину роботи може здійснюватися відправлення 330 пакетів, або близько 13 Кб даних. Такі дії можуть призвести до зменшення терміну служби акумулятора датчика чи пристрою на умовні 54 хвилини та зайняти ефірний час при відправці 330 сигнальних подій;
- якщо вузол передає дані протягом інтервалу, що дорівнює умовно п’яти секундам, це призводить до постійного активного використання мережевих ресурсів. За цей проміжок часу, може передаватися 720 пакетів або 28,8 Кб за одну годину, що потребує 60 хвилин роботи акумулятора та надсилання лише одного сигнального повідомлення;
- якщо смуга пропускання нераціонально використовується, це може призвести до значного навантаження на ресурси для завантаження значних за розміром файлів. Наприклад, для завантаження відеоматеріалів розміром понад 1 Гб, при умовній швидкості 1,5 Мбіт/с, потрібно не менше 1,5 години безперервних сесій високочастотного зв’язку.

Тому важливо досліджувати та розробляти підходи для зменшення ризиків неефективного використання ресурсів, зокрема впровадження енергоефективних протоколів та механізмів захисту, що забезпечують безперервну роботу мережі, особливо у випадку аномалій чи загроз [5].

ДОСЛІДЖЕННЯ ПРИРОДИ ЗБОЇВ ТА ВІДМОВ В СЕНСОРНИХ МЕРЕЖАХ

Коли досліджується природа збоїв працездатності вузлів сенсорної мережі, доцільно підкреслити, що у деяких випадках, помилка в роботі програмного забезпечення може призвести до масового збою всієї мережі. Тому заведено розмежовувати рівні збоїв за наступними категоріями:

Збої у роботі вузла. Через те, що сенсорні елементи (вузли) мають у своєму складі кілька апаратних і програмних компонентів, вони своєю чергою, можуть викликати несправності. Наприклад, вплив негативних чи подекуди екстремальних чинників навколишнього середовища (пошкодження корпусу вузла, короткі замикання від впливу води тощо). Доцільно підкреслити, що наближення розріджування енергоносіїв також може вплинути на коректну роботу вузла (неточні зчитування показників задимленості,

вологи, наявності ворожого БПЛА в зоні впливу тощо). Як висновок, апаратні збої призводять до програмних.

Однак, навіть якщо сенсорний вузол тимчасово не здатен зчитувати та первинно опрацьовувати певні показники, він може успішно брати участь у ретрансляції та маршрутизації даних від сусідніх вузлів. Під час пересилання повідомлень вузли мають можливість агрегувати дані з кількох інших елементів мережі для зменшення кількості інформації, що надсилається на базову станцію. Якщо вузол генерує неправильну інформацію, результати агрегування даних можуть відхилятися від реальних, достовірних значень. Також, якщо вузол, відповідальний за генерування агрегованих даних, піддається збою чи негативному впливу зловмисника, базова станція отримає неправильну інформацію про весь сегмент сенсорної мережі. Такі дані можуть вважатися скомпрометованими [6].

Збої у роботі мережі. Оскільки при проєктуванні сенсорних мереж, зв'язність та ретрансляція даних являється одними із основних завдань, до процесу маршрутизації висувається низка вимог. Маршрутизація необхідна для збору даних з сенсорів, для регулярного пошуку альтернативних маршрутів, для розповсюдження оновлень програмного забезпечення та конфігурацій, а також для здійснення постійної координації між вузлами.

Також варто зазначити, що серйозні вимоги щодо безпечної та безвідмовної роботи покладаються і на специфічні протоколи маршрутизації, наприклад, для військових застосувань при відстеженні або супроводу рухомих об'єктів (БПЛА).

У сенсорній мережі зв'язки між вузлами не завжди стабільні. Радіозавади часто призводять до некоректної роботи мережі. В інших ситуаціях вузли можуть мати ідеальний зв'язок, але пакети не доставляються до місця призначення через помилки маршрутів. Це призводить до постійних змін у виборі оптимальних маршрутів, появи петель, відмов в обслуговуванні, виходу з ладу вузлів, або доставленні повідомлень до нелегітимних (неправильних) місць призначення.

Як результат, збої у коректній роботі маршрутизації частіше за все можуть призводити до втрат пакетів, недоцільного використання енергоресурсів, затримок при опрацюванні запитів або неправильного пересилання даних [7].

Збої у роботі приймачів. Приймальна сторона відповідальна за збір даних, що генеруються у мережі, та передавання їх до центрів обробки. Тому вона також піддається збоям.

При умові виході з ладу приймача (базової станції), якщо архітектурою мережі не передбачені альтернативні (допоміжні) маршрути або інші засоби відмовостійкості, відбувається масовий збій роботи сенсорної мережі. Дані від сенсорних вузлів не можуть бути отримані та опрацьовані. Також топологією мережі може бути реалізоване розгортання приймача в районах, де відсутнє постійне електроживлення, що також може призвести до поступового погіршення підключення та зв'язку [8].

В таких випадках доцільно запропонувати використання батареї разом із сонячними панелями для забезпечення необхідно рівня живлення. Крім цього, негативний плив може бути спрямований і на програмне забезпечення приймача. В цьому варіанті, зібрані з мережі дані, також вважаються скомпрометованими, що може призвести до втрати даних у період, коли відбулася атака чи стався збій [9].

ISSN 2663 - 4023

РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ

Як показує дослідження природи збоїв, відмовостійкість та безпека в сенсорних мережах взаємопов'язані, та формують узагальнену структуру надійної системи, яка здатна витримувати як внутрішні збої та відмови, так і зовнішні загрози чи деструктивні впливи зловмисників [10].

Для прикладу зв'язку відмовостійкості та безпеки доцільно розглянути сенсорну мережу, в якій використовуються 50, 100, 200 та 500 вузлів. Якщо елементи мережі працюють незалежно, то при цьому ймовірність того, що всі елементи в мережі працюють без відмов та збоїв буде дорівнювати: $(1-p)^n$.

Доцільно припустити, що ймовірність відмови кожного вузла протягом певного періоду складатиме 0.01 (1%). Ймовірність, що жоден вузол не відмовить, можна розрахувати за формулою:

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

де n — це кількість елементів сенсорної мережі.

Для 50 вузлів ймовірність, що всі вузли працюватимуть без відмов, становить приблизно 60,5%; для 100 вузлів — ймовірність знижується до 36,6%; для 200 вузлів — 13,4%, а для 500 вузлів ймовірність становить лише 0,66%.

На рис. 1. 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, алгоритми толерантності до помилок тощо [11]. Особливо коли мова йде про проєктування мереж зі значно більшою кількістю сенсорних вузлів.

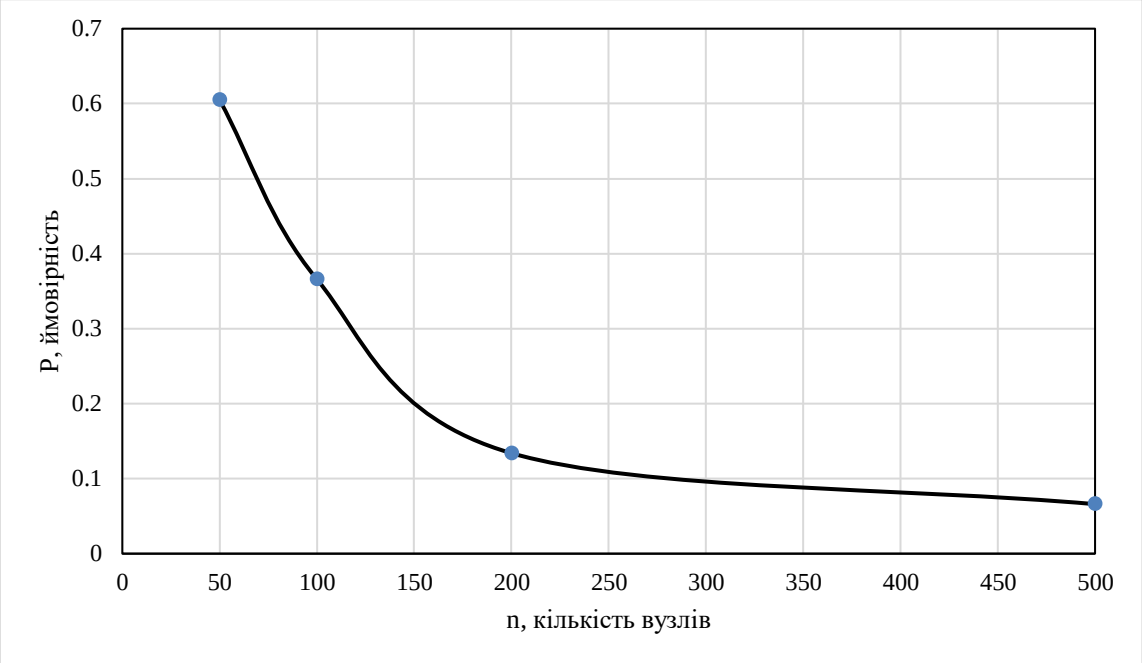

Рис. 1. Вплив зміни кількості вузлів на ймовірність відмови сенсорної мережі

Для ситуації, коли потрібно провести моделювання впливу зловмисника на сенсорну мережу, можна розглянути та проаналізувати різні сценарії атаки. Наприклад, сценарії можуть бути у вигляді атак jamming, атак на створення колізій, атак виснаження ресурсів вузлів мережі, або ж атаки на протоколи маршрутизації чи DoS (DDoS) атаки [12].

Сенсорні мережі також вразливі до атак перехоплення та аналізу трафіку, що дозволяє зловмисникам отримати доступ до даних, здійснювати модифікацію конфіденційних даних чи підміну легітимності прав для подальшого негативного впливу на мережу й інші елементи. Доцільно запроваджувати покращенні методи шифрування та автентифікації для забезпечення конфіденційності і цілісності даних.

Припускається, що при моделюванні DoS атаки зловмисник робить спробу вивести з ладу певну кількість вузлів СМ. Відомо, що це може призвести до зниження загальної ймовірності безвідмовної роботи мережі. Тому ймовірність, що мережа продовжить функціонувати без відмов, можна оцінити за формулою:

$$P = (1-p)^{n-a} * (1-q)^{a}, \quad (2)$$

де P — базова ймовірність відмови вузла без зовнішнього впливу, n — загальна кількість вузлів у мережі, a — кількість вузлів, які зловмисник успішно атакував, q — ймовірність, що зловмисник зможе вивести з ладу вузол.

Якщо припустити, що ймовірність відмови кожного вузла P дорівнює 1%, кількість вузлів в мережі n — 100, кількість вузлів під атакою a буде дорівнювати 20, а ймовірність успішної атаки на вузол q — 50%, то за заданими параметрами, ймовірність безвідмовної роботи мережі в умовах атаки дуже мала і становить приблизно $4{,}27 * 10^{-7}$.

Розраховане значення демонструє вплив, який атака може мати на надійність сенсорної мережі. Результат демонструє критичну необхідність розробки механізмів для захисту мережі від зловмисних атак, а також підтверджує важливість впровадження стратегій для підвищення функціональної стійкості, таких як резервування і відновлення вузлів.

Ймовірність безвідмовної роботи без втручання зловмисника (P_k) розраховується за наступною формулою:

$$P_k = (1-p)^{n}. \quad (3)$$

Враховується ймовірність, що жоден з вузлів мережі не відмовить, і працюватиме з необхідним рівнем відмовостійкості. При цьому значення кількості вузлів, що знаходяться під атакою можна наступним чином:

$$n_a = \lceil n * a \rceil. \quad (4)$$

Ймовірність безвідмовної роботи з втручанням зловмисника (P_f) можна розрахувати:

$$P_f = (1-p)^{n-a} * (1-q)^{a}. \quad (5)$$

Враховується ймовірність того, що вузли, які не атаковані, продовжують працювати у звичайному режимі, не відмовлять, а також ймовірність того, що атаковані вузли також продовжуватимуть працювати, однак інформація, яку вони передають, можна вважати скомпрометованою.

Наприклад, значення ймовірностей для сенсорної мережі із кількістю елементів, що дорівнює 100, буде наступною:

- без атаки: $P_k = (1-0{,}01)^{100} \approx 0{,}366$;
- з атакою (якщо припустити, що 10 вузлів було атаковано): $P_f = (1-0{,}01)^{90} * (1-0{,}5)^{10} \approx 0{,}025$.

Зі збільшенням кількості вузлів, ймовірності безвідмовної роботи без втручання зловмисника будуть наступними: для 10 вузлів ≈ 0.904, для 50 вузлів ≈ 0.605, для 200 вузлів ≈ 0.134, та для 500 вузлів ≈ 0.007.

ISSN 2663 - 4023

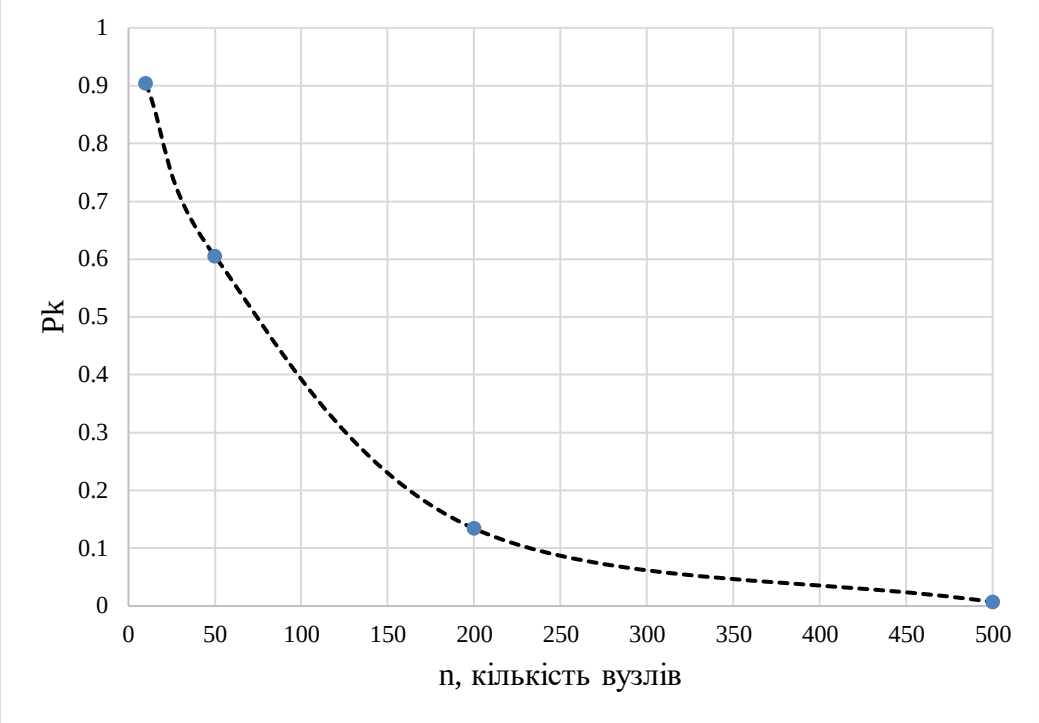

Рис. 2. Ймовірність безвідмовної роботи сенсорної мережі зі збільшенням кількості вузлів

При цьому зі збільшенням кількості вузлів, ймовірності безвідмовної роботи з втручанням зловмисника будуть наступними: для 10 вузлів (при 1 атакованому вузлі) приблизно дорівнює 0.457, для 50 вузлів (при 5 атакованих вузлах) ≈ 0.020, для 200 вузлів (при 20 атакованих вузлах) приблизно дорівнює $1{,}56 * 10^{-7}$, та для 500 вузлів (при 50 атакованих вузлах) приблизно $9{,}65 * 10^{-18}$.

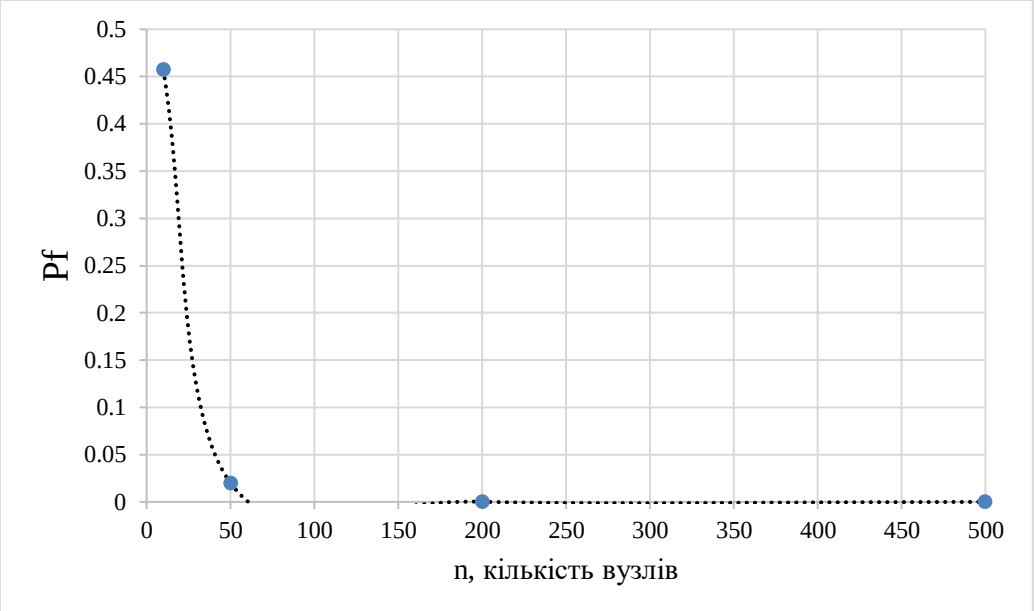

Рис. 3. Порівняння ймовірностей безвідмовної роботи сенсорної мережі в умовах зміни кількості атакованих вузлів

Результати розрахунків, приведені на рис. 2 та рис. 3 демонструють, як ймовірність безвідмовної роботи зменшується із збільшенням кількості вузлів і як значно погіршується ситуація при втручанні зловмисника [13].

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Враховуючи стрімкий розвиток та впровадження сенсорних мереж в різноманітні сфери та галузі людського життя, необхідним є проведення дослідження відмовостійкості та енергоефективності сенсорних мереж.

В процесі дослідження було встановлено, що відмовостійкість сенсорної мережі значно знижується зі збільшенням кількості вузлів, особливо у випадках аномальної поведінки окремих вузлів чи груп вузлів, а також при втручанні зловмисників. Це підтверджується розрахунками ймовірності безвідмовної роботи, які показали суттєве зменшення показників надійності при збільшенні числа атакованих вузлів.

Варто підкреслити, що питання оптимізації споживання енергоресурсів залишається важливим, а іноді й критичним аспектом для забезпечення довготривалої роботи сенсорних вузлів.

Надалі доцільно зосередити увагу та зусилля науковців на створенні та впровадженні протоколів, які здатні мінімізувати енергоспоживання вузлів, при цьому, як наслідок, підвищити автономність. Також питання вдосконалення чинних та розробка нових механізмів захисту від зловмисних втручань, атак DoS (DDoS) потребують значної частки уваги, що своєю чергою, забезпечить підвищення надійності та стійкості сенсорних мереж.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 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.
2. Liu, D., & Ning, P. (2007). *Security for Wireless Sensor Networks.* Springer. https://doi.org/10.1007/978-0-387-46781-8
3. Adday, G. H., Subramaniam, S. K., Zukarnain, Z. A., & Samian N. (2022). Fault Tolerance Structures in Wireless Sensor Networks (WSNs): Survey, Classification, and Future Directions. *Sensors, 22(16), 6041.* https://doi.org/10.3390/s22166041
4. Dovzhenko, N., Barabash, O., Ausheva, A., Ivanichenko, Y., & Obushnyi, S. (2023). Comprehensive Analysis of Efficiency and Security Challenges in Sensor Network Routing. *Cybersecurity Providing in Information and Telecommunication Systems, CPITS-II 2023, Vol. 3550,* 275–280.
5. Choudhary, A., Kumar, S., Gupta, S., Gong, M., & Mahanti, A. (2021). FEHCA: A Fault-Tolerant Energy-Efficient Hierarchical Clustering Algorithm for Wireless Sensor Networks. *Energies, 14(13), 3935.* https://doi.org/10.3390/en14133935
6. Mehrotra, D., Srivastava, R., Nagpal, R., & Nagpal, D. (2020). Multiclass classification of mobile applications as per energy consumption. *Journal of King Saud University-Computer and Information Sciences, 32(10),* 1204–1205. https://doi.org/10.1016/j.jksuci.2018.05.007
7. 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, 5(3),* 255–272. https://doi.org/10.46328/ijonest.174
8. Perrig, A., Stankovic, J., & Wagner, D. (2004). Security in wireless sensor networks. *Communications of the ACM, 47(6),* 53–57. https://doi.org/10.1145/990680.990707
9. Sowndeswari, S., Kavitha, E., & Krishnamoorthy, R. (2024). Enhancing security in wireless sensor networks: A fusion of deep learning and energy-efficient routing. *Journal of Intelligent & Fuzzy Systems.* https://doi.org/10.3233/JIFS-235322

10. Karpenko, A., Bondarenko, T., Ovsiannikov, V., & Martyniuk, V. (2020). Ensuring information security in wireless sensor networks. *Electronic Professional Scientific Journal "Cybersecurity: Education, Science, Technique", 2(10),* 54–66. https://doi.org/10.28925/2663-4023.2020.10.5466
11. Jain, U., & Hussain, M. (2018). Wireless Sensor Networks: Attacks and Countermeasures. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3170185
12. 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
13. Barabash, O., Ausheva, N., Dovzhenko, N., Obidin, D., Musienko, A., & Fedchuk, T. (2023). Development of a hybrid network traffic load management mechanism using smart components. *7th International Conference on Methods and Systems of Navigation and Motion Control (MSNMC),* 38–41.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (24), 2024
ISSN 2663 - 4023

Oleh Barabash
Doctor of Technical Sciences, Professor, Professor of the
Department of Software Engineering in Energy
National Technical University of Ukraine «Igor Sikorsky
Kyiv Polytechnic Institute», Kyiv, Ukraine
ORCID ID: 0000-0003-1715-0761
bar64@ukr.net

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

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

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

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

TECHNICAL ASPECTS OF BUILDING A FAULT-TOLERANT SENSOR NETWORK INFRASTRUCTURE

Abstract. This article examines the features and application areas of sensor networks, including environmental monitoring, military applications, smart building management, and smart cities. The necessity of ensuring fault tolerance and energy efficiency of network elements is analyzed. It is noted that modern sensor networks can autonomously respond to changes in the deployment and operation environment, maintaining functionality even in case of failures and disruptions. Various methods for ensuring fault tolerance are studied, including the use of self-configuration algorithms, role rotation among sensors, hierarchical node management systems, and others. The need for developing new and improving existing energy-efficient protocols that minimize energy consumption of individual nodes and enhance the autonomy and reliable functioning of sensor network segments is emphasized. The impact of decreasing and increasing the number of nodes on network fault tolerance and their ability to self-recover under abnormal and malicious interference conditions is analyzed. The necessity of improving protection mechanisms against such interferences to enhance network reliability and stability is highlighted. The consequences of the growing impact of new threats and vulnerabilities on the security of sensor networks are separately

emphasized, requiring constant monitoring, search for reliable and productive solutions, updates, and improvements to protection mechanisms. Additionally, adaptive algorithms for resource and traffic management capable of quickly responding to changing operating conditions and preventing information security anomalies are analyzed. Achieving high levels of fault tolerance and energy efficiency in sensor networks is noted as a key factor for their successful use in critical applications. Prospects for further research in the field of energy efficiency and fault tolerance of sensor networks are analyzed.

Keywords: sensor network; security; fault tolerance; threats; anomalies; reliability; nodes; UAV.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Barabash, O. V., Dovzhenko, N. M., & Ausheva, N. M. (2024). Intehrovanyi pidkhid do zabezpechennia bezpeky v sensornykh merezhakh. *XI Vseukrainska naukovo–praktychna konferentsiia molodykh uchenykh,* 223–224.
2. Liu, D., & Ning, P. (2007). *Security for Wireless Sensor Networks.* Springer. https://doi.org/10.1007/978-0-387-46781-8
3. Adday, G. H., Subramaniam, S. K., Zukarnain, Z. A., & Samian N. (2022). Fault Tolerance Structures in Wireless Sensor Networks (WSNs): Survey, Classification, and Future Directions. *Sensors, 22(16), 6041.* https://doi.org/10.3390/s22166041
4. Dovzhenko, N., Barabash, O., Ausheva, A., Ivanichenko, Y., & Obushnyi, S. (2023). Comprehensive Analysis of Efficiency and Security Challenges in Sensor Network Routing. *Cybersecurity Providing in Information and Telecommunication Systems, CPITS-II 2023, Vol. 3550,* 275–280.
5. Choudhary, A., Kumar, S., Gupta, S., Gong, M., & Mahanti, A. (2021). FEHCA: A Fault-Tolerant Energy-Efficient Hierarchical Clustering Algorithm for Wireless Sensor Networks. *Energies, 14(13), 3935.* https://doi.org/10.3390/en14133935
6. Mehrotra, D., Srivastava, R., Nagpal, R., & Nagpal, D. (2020). Multiclass classification of mobile applications as per energy consumption. *Journal of King Saud University-Computer and Information Sciences, 32(10),* 1204–1205. https://doi.org/10.1016/j.jksuci.2018.05.007
7. 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, 5(3),* 255–272. https://doi.org/10.46328/ijonest.174
8. Perrig, A., Stankovic, J., & Wagner, D. (2004). Security in wireless sensor networks. *Communications of the ACM, 47(6),* 53–57. https://doi.org/10.1145/990680.990707
9. Sowndeswari, S., Kavitha, E., & Krishnamoorthy, R. (2024). Enhancing security in wireless sensor networks: A fusion of deep learning and energy-efficient routing. *Journal of Intelligent & Fuzzy Systems.* https://doi.org/10.3233/JIFS-235322
10. Karpenko, A., Bondarenko, T., Ovsiannikov, V., & Martyniuk, V. (2020). Ensuring information security in wireless sensor networks. *Electronic Professional Scientific Journal "Cybersecurity: Education, Science, Technique", 2(10),* 54–66. https://doi.org/10.28925/2663-4023.2020.10.5466
11. Jain, U., & Hussain, M. (2018). Wireless Sensor Networks: Attacks and Countermeasures. *SSRN Electronic Journal.* https://doi.org/10.2139/ssrn.3170185
12. 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
13. Barabash, O., Ausheva, N., Dovzhenko, N., Obidin, D., Musienko, A., & Fedchuk, T. (2023). Development of a hybrid network traffic load management mechanism using smart components. *7th International Conference on Methods and Systems of Navigation and Motion Control (MSNMC),* 38–41.

(cc) BY-NC-SA

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