КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА
ФАКУЛЬТЕТ РАДІОФІЗИКИ, ЕЛЕКТРОНІКИ ТА КОМП'ЮТЕРНИХ СИСТЕМ

Кафедра радіотехніки та радіоелектронних систем

«На правах рукопису»

Робота допущена до захисту в ЕК
рішенням кафедри радіотехніки та радіоелектронних систем
від _____ року, протокол №____.
Завідувач кафедри доктор фіз.-мат. наук, професор
_____ Ігор АНІСІМОВ

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА
на тему:
"ПОБУДОВА АДАПТИВНИХ СЕНСОРНИХ МЕРЕЖ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЇХ ЗВ'ЯЗАНОСТІ В УМОВАХ ЗАВАДОВОЇ ОБСТАНОВКИ ТА КІБЕРВПЛИВІВ"

Виконав:
студент 4-го курсу
денної форми навчання
спеціальності 172 – Електронні комунікації та радіотехніка
ОПП «Інформаційна безпека телекомунікаційних систем і мереж»
Гиленко Сергій Андрійович _____

Науковий керівник:
доцент кафедри радіотехніки
та радіоелектронних систем
Гахович Сергій Вікторович _____

Рецензент:
начальник наукового відділу
науково-дослідного центру ВІ КНУ
Лоза Віталій Миколайович _____

Засвідчую, що у цій бакалаврській роботі
немає запозичень з праць інших авторів без
відповідних посилань
Студент _____Сергій Гиленко

Київ - 2025

РЕФЕРАТ

Дипломна робота: 45 с., 2 табл., 17 рис., 1 дод. (6 с.), 7 джерел.

СЕНСОРНА МЕРЕЖА, КІБЕРБЕЗПЕКА, ЗВ'ЯЗАНІСТЬ, ЗАВАДИ, КІБЕРВПЛИВ, АДАПТИВНІСТЬ, МАРШРУТИЗАЦІЯ.

Об’єкт дослідження – адаптивні сенсорні мережі. Мета роботи – побудова адаптивних сенсорних мереж для забезпечення їх зв'язаності в умовах завадової обстановки та кібервпливу. Розроблено підхід до побудови адаптивних сенсорних мереж, який враховує умови завадової обстановки та кібервпливу. Проаналізовано існуючі методи та протоколи маршрутизації в сенсорних мережах з урахуванням загроз та особливостей їх функціонування в деструктивному середовищі. Запропоновано механізми підвищення стійкості зв'язку та забезпечення зв'язаності мережі за наявності зовнішніх впливів. Завдяки розробці та впровадженню адаптивних алгоритмів функціонування, включаючи механізми виявлення та протидії завадам і кіберзагрозам, вдалось досягнути високого рівня надійності передачі даних та збереження працездатності мережі навіть в умовах інтенсивних зовнішніх впливів. Запропоновані рішення дозволяють забезпечити безперервне функціонування сенсорних мереж, що є критично важливим для моніторингу та управління в складних і небезпечних середовищах. Розроблена система може бути використана для підвищення безпеки та надійності існуючих сенсорних мереж, а також при проектуванні нових систем, що працюють в умовах високих ризиків. У подальшому слід вдосконалити алгоритми адаптації мережі до динамічно змінних умов, зокрема за рахунок інтеграції елементів штучного інтелекту для прогнозування та попередження загроз.

ЗМІСТ

Перелік умовних скорочень та позначень

БСМ - Бездротові сенсорні мережі
РЕБ - Засоби радіоелектронної боротьби
ІВ - Інформаційні вузли
СМ - Сенсорні мережі

ВСТУП

Стрімкий розвиток інформаційно-комунікаційних технологій, зокрема бездротових сенсорних мереж (БСМ), призвів до масштабних змін у підходах до збору, передачі та обробки даних у реальному часі. Бездротові сенсорні мережі — це один із ключових елементів сучасних кіберфізичних систем, який дозволяє здійснювати моніторинг середовища, керування технічними об'єктами, захист критичної інфраструктури та оперативне реагування на надзвичайні ситуації. У військовій справі, безпеці, охороні довкілля та енергетиці такі мережі стають інструментом критичного значення.

На фоні постійного ускладнення сучасних конфліктів, широкого застосування засобів радіоелектронної боротьби і високого рівня кіберзагроз, сенсорні мережі повинні зберігати зв’язок навіть в умовах цілеспрямованих зовнішніх впливів. Саме тому з’являється потреба у побудові адаптивних сенсорних мереж, здатних ефективно функціонувати в умовах кібервтручання.

Актуальність дослідження обумовлена тим, що більшість існуючих архітектур сенсорних мереж не здатні забезпечити гарантовану передачу даних у складному середовищі з високим рівнем завад та атак. Типові протоколи маршрутизації можуть втратити ефективність, коли структура мережі постійно змінюється через знищення або пошкодження вузлів, заглушення або хакерські втручання. У таких умовах необхідно створити нові методи маршрутизації, які враховують змінність середовища та здатні оперативно перебудовувати маршрути без втрати зв’язку з критичними вузлами.

Метою дипломної роботи є розробка методу побудови адаптивних сенсорних мереж, який забезпечує збереження зв’язаності мережі у складних умовах, включаючи руйнівні кібервпливи та навмисні радіоперешкоди. Досягнення цієї мети передбачає вирішення комплексу задач, пов’язаних з аналізом

типових завад, вибором ефективної топології мережі, реалізацією динамічних протоколів маршрутизації, а також впровадженням засобів самодіагностики та самовідновлення мережі.

Сучасний стан досліджень у галузі побудови сенсорних мереж зосереджено навколо протоколів типу AODV, DSR, LEACH, які здатні працювати у стандартному безпечному середовищі, проте не адаптовані до специфіки роботи у середовищі з високим рівнем загроз. Окремі наукові дослідження вже торкаються аспектів динамічного маршрутизування з урахуванням завад, однак практичне впровадження таких підходів обмежене складністю їх реалізації або недостатньою стійкістю до кібератак.

Наукова новизна полягає у створенні комплексного методу побудови мережі, який включає алгоритми адаптації топології мережі в режимі реального часу, аналіз загроз, використання механізмів самодіагностики та впровадження систем захисту інформації. Унікальність підходу полягає в інтеграції засобів радіоелектронного моніторингу із механізмами адаптивного реагування на виявлені зміни в середовищі функціонування.

Значущість розробки визначається її застосовністю в критичних галузях — оборона, енергетика, надзвичайні ситуації, де від надійності зв’язку залежить ефективність прийняття рішень. Запропонований підхід дозволяє істотно підвищити живучість мережі, її енергоефективність та здатність до автономної роботи за умови бойових дій та різного рівня катастроф

Проблематика галузі охоплює широке коло завдань: нестабільність каналів зв’язку, обмеження енергоресурсів, складність динамічного перепланування маршрутів, а також постійні загрози з боку кібератак

РОЗДІЛ 1. АНАЛІЗ І ОЦІНКА ОСОБЛИВОСТЕЙ ФУНКЦІОНУВАННЯ СЕНСОРНИХ МЕРЕЖ В УМОВАХ ЗАВАДОВОЇ ОБСТАНОВКИ ТА КІБЕРВПЛИВУ

1.1 Підходи до застосування сенсорних мереж арміями світу

У сучасних умовах розвитку військових технологій сенсорні мережі відіграють ключову роль у забезпеченні ситуаційної обізнаності, спостереження та захисту військових об’єктів. Передові країни світу, такі як США, Велика Британія, Німеччина, Ізраїль, Китай, Туреччина та Франція, активно впроваджують ці технології у свої оборонні стратегії, і кожна з них має свої унікальні підходи до використання сенсорних мереж.

США мають найрозвиненішу систему використання сенсорних технологій у військовій сфері. Вони активно застосовують бездротові сенсорні мережі (WSN) для розвідки, виявлення цілей, контролю периметра та управління військами. Особливо варто зазначити використання сенсорів у складі системи "Future Combat Systems" (FCS), яка передбачала повну інтеграцію сенсорів із бойовими машинами та інформаційними мережами [9, с. 25]. Крім того, широко використовуються сенсорні платформи типу WISDOM і SAND, які забезпечують довготривале розміщення в бойових зонах із можливістю автономного збору та передачі інформації через супутникові канали [16 с. 19].

Велика Британія активно впроваджує сенсорні мережі для прикордонного контролю, а також у морських операціях. У рамках програми NITEworks британське Міністерство оборони розробляє моделі застосування сенсорних мереж у бойових сценаріях для реального часу [3, с. 41]. Відомою є система WATCHKEEPER, яка інтегрує сенсорні дані з БПЛА, наземними системами та мобільними модулями для моніторингу [5 с. 33].

Німеччина зосереджена на розвитку інтегрованих сенсорних платформ для бронетанкових і піхотних підрозділів. Проект “Infanterist der Zukunft” (Солдат

майбутнього) включає використання персональних сенсорів для контролю за життєвими показниками військових, моніторингу місцевості та комунікації з командними пунктами [9, с. 29]. Відомі також дослідження Бундесверу у сфері адаптивних сенсорних систем для оборони об'єктів.

Ізраїль — одна з лідерів у застосуванні сенсорних мереж у сфері протидії терористичним загрозам. Військові застосовують розгалужені мережі сенсорів уздовж кордонів, зокрема з Сектором Газа, для виявлення підземних тунелів і несанкціонованого проникнення. Компанія Rafael та Ізраїльська оборонна компанія Elbit Systems розробили комплексні рішення на основі сенсорів, які можуть взаємодіяти з безпілотниками та автономними бойовими модулями [3, с. 44]. Особливою популярністю користуються мобільні сенсорні вузли, що діють у мережевій архітектурі з автоматичною обробкою даних.

Китай використовує сенсорні мережі не тільки в рамках звичайних військових систем, але і для підтримки концепції "інтелектуального поля бою". Китайська армія розробляє технології "розумного батальйону", в якому кожен елемент озброєння та спорядження має інтегровані сенсорні модулі для збору даних про середовище, противника та стан військовослужбовця [5, с. 38]. Військові дослідницькі інститути КНР активно вивчають мультиагентні сенсорні системи для автономного реагування на загрози [16, с. 23].

Туреччина зосередилася на використанні сенсорних мереж у поєднанні з автономними системами — зокрема з безпілотниками Bayraktar TB2. У зоні конфліктів на Близькому Сході турецька армія застосовувала мобільні сенсорні вузли, що синхронізуються з артилерією та авіацією. Туреччина також розробляє власні системи раннього попередження на основі сенсорних даних для оборони критичних інфраструктур [9, с. 32].

Франція у межах проекту SCORPION активно розробляє мережево-центричні технології, що інтегрують сенсорні вузли, транспортні засоби, дрони та інші

платформи в єдине цифрове бойове середовище. Сенсори використовуються для спостереження, навігації, розвідки та точного наведення артилерії [5, с. 36]. Особливий акцент робиться на мікросенсорних платформах, які можуть розміщуватись у складних умовах і передавати дані в реальному часі.

1.2 Аналіз структури та особливостей поширення інформації в безпроводових сенсорних мережах

Безпроводові сенсорні мережі є складними розподіленими системами, які складаються з великої кількості вузлів (сенсорів), здатних до вимірювання фізичних величин навколишнього середовища, обробки інформації та її передачі до центрального вузла чи базової станції. У БСМ кожен сенсор має обмежені ресурси – енергію, обчислювальну здатність, пам’ять та радіус дії, що зумовлює специфіку структурної організації мережі та методів передачі даних.Структура та опис БСМ наведені у таблиці 1.1.

Таблиця 1.1 Структура БСМ

Назва	**Опис**
Плоскі (однорангові) мережі	Усі вузли функціонально однакові. Дані передаються багатоетапним маршрутом від вузла до вузла до центрального шлюзу. Така структура проста у реалізації, однак має обмежену масштабованість та енергетичну ефективність.
Ієрархічні (кластеризовані) мережі	окремі вузли (кластерні голови) відповідають за збір інформації від підлеглих сенсорів і передачу її далі. Це дозволяє зменшити кількість

	транзакцій, знизити навантаження на мережу та оптимізувати енергоспоживання
Гібридні структури	Поєднують переваги плоскої та ієрархічної архітектури, забезпечуючи гнучкість і масштабованість.

У БСМ існує кілька моделей розповсюдження інформації:

1. Data-centric routing — передача відбувається на основі змісту (запит – відповідь), а не на основі ідентифікаторів вузлів.
2. Query-based routing — дані надсилаються у відповідь на конкретні запити користувача.
3. Negotiation-based protocols — використовують узгодження між вузлами перед надсиланням даних, щоб уникнути надмірної дублюваної інформації.
4. Location-based routing — використовує інформацію про місце розташування вузлів для визначення маршрутів передачі даних.

Ці моделі дають змогу зменшити енергоспоживання, підвищити масштабованість мережі та забезпечити збалансоване навантаження між вузлами.

Передача інформації у БСМ має низку особливостей, які випливають з обмеженості ресурсів:

Енергозбереження – ключовий фактор при проектуванні мережевих протоколів безпроводових систем. Передача даних є найбільш енерговитратною операцією. Тому застосовуються алгоритми агрегації даних (data fusion) на локальних вузлах [8, с. 113].

Надійність та достовірність – через втрати пакетів, інтерференцію та зміну топології через розрядження вузлів, особливо важливо забезпечити маршрутизацію з підтвердженням доставки даних або дублюванням.

Адаптивність маршрутів – враховуючи часту зміну стану мережі, маршрутизатори повинні динамічно обирати оптимальний шлях до базової станції, часто з використанням алгоритмів штучного інтелекту.

Локальність обміну – з метою економії енергії вузли зазвичай взаємодіють лише із сусідніми вузлами, що обмежує швидкість та обсяг обміну інформацією [10, с. 78].

Безпека – конфіденційність, цілісність і автентичність переданих даних потребують особливої уваги, оскільки відкрите радіоефірне середовище піддається загрозам атак.

Окрім цього, топологія мережі може змінюватися у процесі функціонування: вузли виходять з ладу, переміщуються (у мобільних застосуваннях), що вимагає побудови адаптивних самоконфігурованих маршрутів, часто на основі таких протоколів як LEACH, PEGASIS, або TEEN [15, с. 126].

У зв'язку з цим поширення інформації у БСМ найчастіше реалізується у вигляді:

Мультихоп-топологій, коли інформація передається послідовно від вузла до вузла;

Топологій з ретрансляторами – призначеними вузлами, які мають підвищену енергоємність;

Мережевих протоколів зі стисканням та агрегацією – з метою зменшення трафіку.

1.2.1 Будова функціональних інформаційних вузлів (ІВ) першого рівня

Функціональні інформаційні вузли, які називають вузлами першого рівня є базовими елементами безпроводових сенсорних мереж, що безпосередньо взаємодіють із навколишнім середовищем, виконуючи функції збирання, обробки та первинної фільтрації даних. Основна роль ІВ полягає у виявленні фізичних явищ, таких як температура, вологість, вібрації, звук, рух, а також у подальшій передачі отриманих даних до вузлів вищого рівня (кластерних вузлів або базової станції).

ІВ першого рівня зазвичай мають модульну структуру, яка включає такі основні компоненти, що наведені в таблиці 1.2.

Таблиця 1.2 Будова функціональних ІВ першого рівня

Назва	**Опис**
Сенсорний модуль (датчик)	Пристрій, який здійснює перетворення фізичних величин (температури, тиску, освітленості тощо) в електричний сигнал. Залежно від призначення системи, сенсори можуть бути різного типу: аналогові, цифрові, мультисенсорні.
2.Мікроконтролер (обчислювальний модуль)	Відповідає за обробку даних, отриманих із сенсорів, виконує фільтрацію, агрегацію, іноді стискання інформації для зменшення навантаження на канал

	передачі. Він також керує іншими модулями вузла (радіомодулем, енергозберігаючими режимами тощо).
Комунікаційний модуль (радіомодуль)	Забезпечує передачу інформації до інших вузлів мережі або до головного вузла. Найпоширеніші технології зв'язку: IEEE 802.15.4 (ZigBee), Bluetooth Low Energy, Wi-Fi, LoRaWAN. Комунікаційний модуль відіграє ключову роль у підтриманні топології мережі та маршрутизації пакетів.
Енергетичний модуль	Включає джерело живлення (акумулятор, батарея, сонячна батарея) та системи керування енергоспоживанням. У більшості випадків вузли першого рівня мають бути енергоефективними, оскільки працюють в автономному режимі.
Модуль зберігання даних	Пам’ять (часто енергонезалежна), у якій тимчасово зберігаються дані перед передачею, а також зберігається програма керування вузлом.

Ключовими особливостями ІВ першого рівня є:

-малі габарити і маса, що дозволяє їхнє масове розгортання в полі;

-обмежені ресурси — пам'ять, обчислювальна потужність, енергетичний запас;

-висока енергозалежність — оскільки енергія не поповнюється регулярно, модулі мають оптимізувати споживання;

-автономність — вузол здатен самостійно виконувати базові функції без централізованого керування;

-гнучкість у конфігурації — можливість інтегрування різних типів сенсорів для вирішення спеціалізованих задач (наприклад, виявлення руху у військових БСМ).

Залежно від архітектури мережі, ІВ першого рівня можуть працювати в таких режимах:

-витіснення — передача даних відбувається тільки за певних умов (перевищення порогу);

-періодичний моніторинг — дані надсилаються з фіксованим інтервалом часу;

-запит-відповідь — вузол надсилає інформацію лише у відповідь на команду з базової станції.

У військових застосуваннях інформаційні вузли першого рівня відіграють ключову роль у створенні ситуаційної обізнаності на полі бою, виявленні рухомих цілей, моніторингу обстановки навколо об’єктів критичної інфраструктури.

1.3 Аналіз методів ефективної маршрутизації у безпроводових сенсорних мережах

Маршрутизація є ключовим компонентом у функціонуванні безпроводових сенсорних мереж (БСМ), оскільки забезпечує ефективну передачу даних від сенсорних вузлів до базової станції або користувача. Особливості БСМ, такі як обмежені ресурси енергії, обчислювальна потужність, пам’ять, висока щільність вузлів, динамічні зміни топології та вимоги до енергоефективності, вимагають розробки спеціалізованих, надійних і адаптивних алгоритмів маршрутизації.

Маршрутизаційні протоколи в БСМ класифікуються за кількома ознаками: способом побудови маршруту, механізмом прийняття рішень, а також характером трафіку. У таблиці 1.3 подано основні типи маршрутизаційних протоколів.

Таблиця 1.3 - Класифікація протоколів маршрутизації у БСМ

Класифікація	**Типи**
За структурою мережі	Плоскі, Ієрархічні, Географічні
За прийняттям рішень	Централізовані, Розподілені
За типом трафіку	Подієві, Запитувальні, Постійні

Плоска маршрутизація

У плоских мережах усі вузли мають однакову роль. Одним із найвідоміших протоколів цієї категорії є SPIN (Sensor Protocols for Information via Negotiation), який мінімізує надмірну передачу шляхом обміну метаданими

перед фактичною передачею даних. Іншим є Directed Diffusion, що базується на запитах і динамічному формуванні маршрутів, забезпечуючи адаптацію до змін у мережі.

Ієрархічна маршрутизація

Ієрархічні протоколи, такі як LEACH (Low-Energy Adaptive Clustering Hierarchy), базуються на кластеризації вузлів. Кожен кластер має головний вузол, яка збирає та агрегує інформацію від підлеглих вузлів і передає її до базової станції. Це знижує енергоспоживання, однак потребує ротації ролі кластерного голови для збалансування енерговитрат. Протокол TEEN, орієнтований на події, використовує порогові значення **виміряних параметрів (наприклад, температури, тиску, вологості)** для передачі даних, що ще більше економить енергію.

Географічна маршрутизація

Географічні (позиційні) протоколи, як-от GPSR (Greedy Perimeter Stateless Routing), використовують координати вузлів для прийняття рішень про пересилання пакетів. Вузол обирає найближчого сусіда до цільової точки. Переваги такого підходу — простота, масштабованість і незалежність від збереження маршрутної інформації. Протокол GAF (Geographic Adaptive Fidelity) дозволяє відключати вузли без втрати покриття, зберігаючи енергію шляхом поділу всієї території покриття на віртуальні географічні зони (сітки). Кожна така зона повинна бути покрита принаймні одним активним вузлом. Вузли в одній зоні періодично обмінюються інформацією про своє місцезнаходження та енергетичний стан. На основі цієї інформації, а також заданих параметрів покриття, GAF дозволяє деяким вузлам переходити в "сплячий" (low-power) режим, якщо їхня функція покриття вже забезпечена іншими активними вузлами в тій самій або сусідній зоні. Періодично "сплячі" вузли прокидаються, щоб перевірити стан мережі та, за потреби, знову стати

активними, забезпечуючи рівномірне розподілення енергетичного навантаження та підтримуючи необхідне покриття всієї території.

Гібридні підходи

Гібридні протоколи поєднують переваги кількох типів. Наприклад, PEGASIS (Power-Efficient Gathering in Sensor Information Systems) формує ланцюг з вузлів, через який дані послідовно передаються від вузла до вузла, об'єднуючись (агрегуючись) на кожному кроці. Лише один обраний вузол (лідер ланцюга) відповідає за передачу агрегованих даних до базової станції. Це значно зменшує кількість безпосередніх передач до базової станції та дозволяє більш рівномірно розподіляти енергетичне навантаження між вузлами в мережі.

У таблиці 1.4. наведено порівняння основних протоколів маршрутизації за ключовими критеріями.

Протокол	**Тип**	**Переваги**	**Недоліки**
SPIN	Плоский	Уникнення дублювання	Не гарантує доставку
Directed Diffusion	Плоский	Адаптивність, ефективність	Затримка при великих обсягах даних
LEACH	Ієрархічний	Енергоефективність, масштабованість	Потребує синхронізації

TEEN	Ієрархічний	Висока економія енергії	Не підходить для періодичних даних
GPSR	Географічний	Простота, масштабованість	Потреба в координатах вузлів
GAF	Географічний	Збереження енергії	Низька точність у великих мережах
PEGASIS	Гібридний	Мінімізація енерговитрат	Складність побудови ланцюга

Таблиця 1.4 Класифікація протоколів маршрутизації у БСМ

Вибір оптимального протоколу маршрутизації для адаптивних сенсорних мереж, що функціонують в умовах завадової обстановки та кібервпливу, є критично важливим. З огляду на вимоги до забезпечення зв'язаності, стійкості до зовнішніх впливів та енергоефективності, жоден з представлених протоколів не є ідеальним самостійно.

- **Плоскі протоколи** (SPIN, Directed Diffusion) демонструють адаптивність, але можуть бути вразливими до завад і кібервпливу через відсутність централізованого контролю та залежність від поширення запитів, що може бути легко порушено. SPIN не гарантує доставку, а Directed Diffusion може мати затримки.
- **Ієрархічні протоколи** (LEACH, TEEN) забезпечують високу енергоефективність та масштабованість за рахунок кластеризації. LEACH вимагає синхронізації, що може бути складною в умовах кібервпливу, а TEEN не підходить для періодичних даних. Однак, модель кластеризації може бути адаптована для ізоляції пошкоджених ділянок мережі та перенаправлення трафіку.
- **Географічні протоколи** (GPSR, GAF) є простими та масштабованими, але вимагають точних координат вузлів, що не завжди можливо в умовах. GAF ефективно зберігає енергію, але може мати низьку точність у великих мережах. Їхня ефективність може знижуватися при відсутності прямої видимості або при спотворенні позиційних даних внаслідок кібератак.
- **Гібридні протоколи** (PEGASIS) поєднують переваги різних підходів, що дозволяє досягти кращої енергоефективності. Однак, складність їх побудови та адміністрування може бути значною.

Для вирішення завдання побудови адаптивних сенсорних мереж, що забезпечують зв'язаність в умовах завадової обстановки та кібервпливу, доцільним є розробка гібридного підходу, який поєднуватиме елементи ієрархічної організації з механізмами адаптивного управління та відновлення. Такий підхід дозволить:

1. **Кластеризувати мережу** для ефективного управління енергією та локалізації впливу загроз.

2. **Впровадити механізми виявлення аномалій та завад** на різних рівнях (фізичному, канальному, мережевому) для оперативного реагування.
3. **Застосувати адаптивні алгоритми маршрутизації**, що можуть динамічно переконфігуровувати шляхи передачі даних, обходячи пошкоджені або заблоковані ділянки мережі.
4. **Інтегрувати елементи кібербезпеки**, такі як автентифікація, шифрування та моніторинг цілісності даних, для протидії кібервпливу.

Таким чином, у контексті даної роботи, особлива увага буде приділена **розробці та аналізу адаптивних механізмів, які дозволять існуючим протоколам або їх модифікаціям ефективно функціонувати в умовах деструктивного середовища.** Це включатиме дослідження методів підвищення відмовостійкості, впровадження інтелектуальних алгоритмів прийняття рішень на основі поточного стану мережі та зовнішніх впливів.

1.3.1 Метод доставки даних з мінімальною затримкою в сенсорних мережах

Однією з ключових вимог до функціонування БСМ у багатьох критичних застосуваннях (військова справа, медичні системи, промисловий моніторинг) є мінімізація затримки доставки даних від сенсорного вузла до базової станції або обчислювального центру. Затримка (латентність) у передачі даних може спричинити втрату актуальності інформації або навіть загрозу для безпеки, якщо мова йде про системи раннього попередження.

Методи доставки даних з мінімальною затримкою передбачають оптимізацію маршруту з урахуванням кількох параметрів: довжина маршруту, кількість пересилань (hop count), завантаженість каналів зв’язку, залишкова енергія вузлів, наявність перешкод у середовищі. Найпоширенішим підходом є

використання маршрутизації на основі пріоритетів, коли вузли призначають вищий пріоритет для пакетів з чутливою до затримки інформацією (наприклад, сигнал про аварійну ситуацію) [12, с. 25].

Серед українських розробок варто виділити метод QELAR (QoS and Energy Aware Routing), адаптований до умов БСМ, де важливу роль відіграє динамічне балансування між якістю обслуговування (QoS) і рівнем енергоспоживання. Метод дозволяє прогнозувати затримку за рахунок використання черг та часових міток, що передаються разом із пакетом [11, с. 119].

Також вивчається концепція оптимального багатоадресного передавання з використанням обхідних маршрутів у разі виявлення вузлів із високим рівнем затримки або втрати пакетів. Така архітектура передбачає дублювання критичних повідомлень через кілька маршрутів, що дозволяє суттєво зменшити ймовірність загальної затримки [7, с. 102].

У БСМ, що працюють в умовах мобільності (наприклад, військові роботизовані платформи), застосовують адаптивні маршрутизатори з прогнозуванням руху вузлів, які враховують зміни топології в реальному часі, зменшуючи при цьому затримки повторного формування маршрутів [1, с. 134].

1.3.2 Метод ефективної маршрутизації в сенсорних мережах

Під терміном “ефективна маршрутизація” у БСМ зазвичай мають на увазі здатність мережі передавати дані з найменшими витратами енергії, затримкою та втратами пакетів, підтримуючи стабільну якість передачі впродовж тривалого часу. Оскільки вузли сенсорної мережі, як правило, живляться від батарей, ефективність маршрутизації напряму пов’язана з тривалістю життя всієї мережі.

Найбільш поширеними у вітчизняних наукових працях визнано три класи методів:

1. Маршрутизація на основі кластеризації (наприклад, алгоритм LEACH), де сенсорні вузли організовуються в кластери з вибором "голови" — вузла, відповідального за збір і пересилання інформації. В Україні активно досліджується модифікований варіант цього методу, зокрема адаптивна кластеризація з урахуванням залишкової енергії вузлів та їхньої відстані до базової станції [4, с. 58].
2. Географічна маршрутизація – використовується, коли вузли мають можливість визначати свої координати (GPS або локальні системи). Дані передаються найкоротшим шляхом у напрямку до базової станції. Однак, дослідники зазначають, що цей метод потребує додаткових витрат на визначення позицій, тому в українських розробках активно розглядається варіант псевдогеографічної маршрутизації за допомогою топологічних координат [2, с. 67].
3. Маршрутизація з урахуванням якості каналу – вузли визначають ефективність передачі на основі параметрів: RSSI, LQI, SNR. Такий підхід дозволяє уникати ділянок із перешкодами або затуханням сигналу, забезпечуючи надійність і довговічність мережі. Одна з актуальних українських реалізацій — метод ETX-маршрутизації (Expected Transmission Count), що дозволяє прогнозувати кількість пересилань для кожного маршруту [14, с. 79].

Додатково розробляються методи з мультиагентною маршрутизацією, де вузли взаємодіють у вигляді кооперативної поведінки, розподіляючи навантаження та вибираючи найефективніші маршрути на основі колективного рішення, що забезпечує баланс між швидкістю та енергоспоживанням [13, с. 90].

1.4 Висновки до першого розділу

У першому розділі було здійснено системний аналіз теоретичних основ, практичних підходів і технічних рішень, що стосуються функціонування БСМ в умовах завадової обстановки та кібервпливу. Детальний розгляд міжнародного досвіду впровадження сенсорних мереж в арміях різних країн сформував висновок, що ці технології стали невід'ємним компонентом сучасного військового управління, розвідки, захисту критичної інфраструктури та обізнаності на полі бою. Найбільш розвиненими в цьому напрямі є США, Велика Британія, Франція, Китай, Ізраїль і Туреччина, де активно впроваджуються інтегровані багаторівневі сенсорні системи, що здатні працювати в умовах радіоелектронного протиборства та адаптуватися до кіберзагроз.

Було проведено аналіз структури БСМ та особливостей поширення інформації в таких мережах. Встановлено, що ключовими особливостями БСМ є обмеженість ресурсів, динамічна топологія, , а також необхідність у побудові маршрутів, що враховують як енергетичні, так і часові параметри. У процесі дослідження структури інформаційних вузлів першого рівня (ІВ-1) з’ясовано, що вони виконують базові функції збору, попередньої обробки, тимчасового зберігання й передачі даних до вищих рівнів, забезпечуючи мінімальну затримку передачі, резервування каналів та шифрування даних.

Окрему увагу було приділено методам маршрутизації у БСМ, зокрема в умовах завад і загроз. Проаналізовано традиційні та новітні підходи до побудови маршрутів, включаючи кластеризацію, географічну маршрутизацію, маршрутизацію з урахуванням якості каналу, мультиагентні системи. Розглянуто сучасні методи зменшення затримки доставки даних, серед яких пріоритетна маршрутизація, адаптивне балансування навантаження, багатоадресне передавання, прогнозування руху вузлів тощо.

У підрозділах 1.3.1 та 1.3.2 систематизовано методи, що дозволяють досягти мінімальної затримки передачі даних та високої енергоефективності. Встановлено, що комплексне використання гібридних алгоритмів маршрутизації з урахуванням топології, динаміки мережі та характеристик передавального середовища є найперспективнішим напрямком подальшого вдосконалення БСМ. Таким чином, отримані результати забезпечують наукову та прикладну базу для формування моделі стійкої та ефективної маршрутизації даних в умовах реальних загроз для БСМ.

РОЗДІЛ 2. АНАЛІЗ ІСНУЮЧИХ ЗАВАД ТА КІБЕРВПЛИВІВ, ЯКІ ВПЛИВАЮТЬ НА РОБОТУ СЕНСОРНИХ МЕРЕЖ

2.1 Характеристики навмисних завад для сенсорних мереж

Сенсорні мережі, які широко застосовуються у військовій справі, охороні стратегічних об'єктів, надзвичайних ситуаціях та інших чутливих сферах, є надзвичайно вразливими до деструктивних впливів, зокрема — до навмисних завад або дій, спрямованих на умисне порушення функціонування системи шляхом передачі перешкод, що призводять до погіршення якості зв’язку, втрати даних або повного виведення з ладу окремих вузлів або мережі в цілому.

Види навмисних завад у сенсорних мережах

Навмисні завади класифікуються залежно від мети впливу, типу використовуваного сигналу та рівня організації атак. Основні типи навмисних завад включають:

Широкосмугові (широкоспектральні) завади – створюються шляхом генерації шуму в усьому діапазоні частот, на яких працює сенсорна мережа. Такі завади ефективні проти мереж, що не мають частотного захисту або механізмів перебудови частоти [17, с. 18].

Нарисні (імпульсні) завади – працюють короткими імпульсами, які зазвичай мають більшу потужність у порівнянні з сигналом мережі. Застосовуються для порушення синхронізації передачі даних [18, с. 45].

Модульовані завади – імітують легітимні сигнали, але мають викривлений зміст або несуть паразитні дані. Їх мета — не тільки порушити передачу, але й ввести систему в оману [19, с. 103].

Цільові завади – спрямовані на конкретний вузол або підмережу з метою її виведення з ладу або обмеження функціоналу (наприклад, вплив на вузли збору даних чи маршрутизатори).

До ключових характеристик навмисних завад належать:

Частотний діапазон впливу – визначає, які частини спектру задіяні для створення завади. Сенсорні мережі часто працюють у діапазонах ISM (наприклад, 2.4 GHz), тому саме ці частоти стають об'єктом завад [20, с. 67].

Рівень потужності завади (Jamming Power) – критичний параметр, що визначає ефективність впливу. Потужні завади здатні блокувати навіть стійкі протоколи передачі, але їх легше виявити.

Тип модуляції завади – визначає, наскільки «схожою» буде завада на легітимний сигнал. Використання однакових схем модуляції зі справжніми пакетами ускладнює виявлення.

Тривалість впливу – завада може бути постійною (періодична передача шуму) або переривчастою (у певні проміжки часу), що ускладнює детекцію [21, с. 49].

Рухливість джерела завади – якщо джерело є мобільним (наприклад, дрон або транспортний засіб), воно може створювати складнощі для систем протидії.

Навмисні завади можуть істотно впливати на різні аспекти роботи сенсорної мережі:

Порушення маршрутизації – зниження ефективності протоколів маршрутизації через втрату пакетів або зміну топології мережі.

Втрата даних – критично важливо для мереж, що передають телеметрію, відео або інші дані в режимі реального часу.

Підвищення енергоспоживання – вузли намагаються повторно передати інформацію або підтримувати зв’язок у складних умовах, що знижує термін їх служби.

Порушення синхронізації – деякі завади спрямовані саме на руйнування часової координації між вузлами.

Протидія навмисним завадам у сенсорних мережах передбачає застосування комплексу технічних, програмних та організаційних заходів, які забезпечують збереження працездатності системи навіть в умовах активного радіоелектронного тиску. Нижче розглянемо основні категорії та технології, що входять до засобів захисту.

1**. Зміна частот передачі (Frequency Hopping Spread Spectrum — FHSS)**

Цей метод передбачає динамічне перемикання робочої частоти відповідно до заздалегідь відомої послідовності. Завдяки цьому зловмиснику значно складніше створити ефективну заваду, оскільки необхідно блокувати весь спектр частот або передбачити перемикання.

Згідно з дослідженнями, FHSS знижує ефективність широкосмугових завад більш ніж на 60% у порівнянні з фіксованим каналом передачі [17, с. 88].

2. **Передача із розширеним спектром (Direct Sequence Spread Spectrum — DSSS)**

Суть цього методу полягає у розширенні сигналу на ширший діапазон за допомогою псевдовипадкової послідовності. Це дозволяє замаскувати сигнал під фоновий шум, роблячи його менш вразливим до навмисного впливу.

Метод DSSS широко використовується в мережах ZigBee та IEEE 802.15.4, які є основою багатьох сенсорних систем [18, с. 69].

3**. Адаптивне управління потужністю**

Один з ключових методів уникнення завад — це автоматичне регулювання потужності передавача залежно від рівня сигналу-шуму (SNR). Це дозволяє зменшити ймовірність виявлення та знищення вузлів.

Використання схем адаптивного регулювання дозволяє зменшити ймовірність успішної атаки більш ніж на 30%, згідно з моделями захисту у роботі [19, с. 54].

4. **Інтелектуальні алгоритми виявлення завад**

Сучасні сенсорні мережі можуть використовувати алгоритми машинного навчання (ML) та штучного інтелекту (AI) для виявлення аномалій у радіоефірі. Наприклад:

класифікація сигналів на "легітимні/шумові";

прогнозування ймовірності появи завад;

активація механізмів обхідного маршруту.

5**. Структурне резервування та маршрутизація**

Впровадження резервних каналів зв'язку та багатоалгоритмічна маршрутизація дозволяють сенсорним мережам оперативно реагувати на втрату вузлів або посилення завад. До таких протоколів належать:

AODV з адаптацією до перешкод;

ZRP з повторними ланцюгами з’єднання;

геоадаптивні протоколи (наприклад, GPSR).

Ці методи дозволяють зберігати цілісність інформаційного потоку навіть при виведенні з ладу 30–50% вузлів [21, с. 40].

2.2 Основні кібератаки та напрямки забезпечення інформаційної безпеки в сенсорних мережах

Сенсорні мережі, які широко використовуються у військовій справі, охороні державного кордону, моніторингу об’єктів критичної інфраструктури, є надзвичайно вразливими до кіберзагроз через свої обмежені обчислювальні ресурси, бездротову передачу даних та відкритість середовища. Забезпечення

інформаційної безпеки в таких мережах передбачає виявлення та запобігання широкому спектру кібератак, серед яких можна виділити найтиповіші. Основны типи кібератак наведені у таблиці 2.1.

Таблиця 2.1 Основні типи кібератак у сенсорних мережах

Атаки на рівні фізичного доступу	**Атаки на мережеву топологію**	**Атаки на передачу даних**	**Атаки на рівень прикладного протоколу**
Фізичне захоплення вузлів (Node Capture) — зловмисник отримує фізичний доступ до сенсорного вузла, витягує з нього ключі шифрування або змінює прошивку. **Підміна вузлів (Node Replication)** — копіювання скомпрометованого вузла і	**Sybil-атака** — зловмисник створює кілька віртуальних ідентичностей вузла в мережі для порушення маршрутизації або накопичення трафіку **Sinkhole-атака** — один вузол видає себе за найбільш оптимальний маршрут і "засмоктує" весь	**Selective forwarding (вибіркове пересилання)** — зловмисний вузол передає лише деякі пакети, що може бути важко виявити. **Hello flood** — зловмисник надсилає потужні сигнали "Hello", примушуючи інші вузли вважати його ближчим, ніж	**Spoofing** — підміна ідентифікаторів вузлів для імітації правомірних учасників мережі. **Data Injection** — впровадження фальшивих

впровадження фальшивих пристроїв у мережу з метою маніпуляцій даними.	трафік, після чого може його змінити або знищити. **Wormhole-атака** — пара скомпрометованих вузлів створює тунель між собою, порушуючи логіку маршрутів і зменшуючи ефективність протоколів.	він є насправді, для порушення структури мережі. **Атака типу DoS (Denial of Service)** — спрямована на перевантаження вузлів або каналів зв’язку, що призводить до втрати продуктивності мережі	даних, що можуть змінити прийняття рішень на рівні командного центру.

Забезпечення інформаційної безпеки в СМ повинно реалізовуватись як на рівні фізичної інфраструктури, так і в каналах передачі даних, системах управління, протоколах маршрутизації, а також на рівні програмного забезпечення й нормативно-організаційних заходів.

1. Фізичний захист вузлів сенсорної мережі

Сенсорні вузли часто розміщуються в неконтрольованому середовищі, що створює загрози несанкціонованого фізичного доступу, демонтажу, підміни

пристроїв. Засобами фізичного захисту є конструктивні рішення (антивандальні корпуси, самознищення даних у разі втручання), використання спеціалізованих сенсорів доступу, застосування камуфляжу або розміщення в охоронюваних зонах.

Для підвищення фізичної безпеки використовуються вбудовані модулі самознищення криптографічної інформації або блокування функцій вузла в разі порушення цілісності корпусу пристрою [26, с. 41].

2. Криптографічні методи захисту інформації

Основою захисту конфіденційності, цілісності та автентичності інформації є криптографія. Через обмеженість ресурсів сенсорних пристроїв перевага надається легковаговим алгоритмам: Tiny Encryption Algorithm (TEA), PRESENT, Lightweight Encryption Algorithm (LEA), а також еліптичній криптографії, яка забезпечує високий рівень безпеки при коротших ключах.

Слід зазначити, що у сенсорних мережах перспективним є використання шифрування на основі еліптичних кривих (ECC), що дозволяє суттєво знизити навантаження на енергоспоживання пристрою при збереженні високого рівня криптостійкості [27, с. 103].

Також важливою є побудова систем розподілу та оновлення ключів: симетричні ключі можуть оновлюватись за допомогою ключових графів, протоколів обміну Diffie–Hellman у модифікованому вигляді, або ж із залученням координатора мережі (шлюзу).

3. Безпечна маршрутизація та топологія

Захист маршрутизації є критичним, оскільки саме цей рівень часто піддається атакам типу "sinkhole", "wormhole", "Sybil", "blackhole". Традиційні протоколи

маршрутизації мають бути доповнені механізмами автентифікації та контролю цілісності маршрутів.

Треба відзначити використання протоколів із багаторівневою перевіркою довіри до вузлів, а також динамічним вибором маршрутів залежно від енергетичного стану та історії поведінки пристрою [28, с. 81].

Додатково впроваджуються резервні маршрути, що дозволяє мережі залишатись функціональною навіть у разі успішної атаки на частину вузлів.

4. Системи виявлення атак (IDS) та запобігання вторгненням (IPS)

У сучасних сенсорних мережах набуває популярності концепція вбудованих систем виявлення атак. Це можуть бути як сигнатурні системи, що порівнюють пакети з відомими шаблонами, так і аномалієві — здатні виявляти нові, ще не задокументовані атаки.

До перспективних підходів належать нейромережеві алгоритми, які дозволяють за допомогою навчання на історичних даних ідентифікувати підозрілу активність із високою точністю [29, с. 93].

Системи IPS (Intrusion Prevention System) можуть не лише виявляти загрозу, а й автоматично змінювати маршрути, блокувати певні вузли, або навіть формувати відповідь на атаку.

5. Захист конфіденційності та цілісності трафіку

Основні механізми захисту даних під час передачі:

End-to-end шифрування – дозволяє уникнути розшифрування на проміжних вузлах;

Використання хеш-функцій та MAC (Message Authentication Code) – забезпечують перевірку цілісності пакету;

Використання nonce (одноразових чисел) або timestamp – для захисту від повторної передачі (replay attack).

Сучасні системи застосовують комбіновані підходи: симетричне шифрування + аутентифікація + часові мітки, що дозволяє створити захищене середовище навіть при наднизькому енергоспоживанні [30, с. 60].

2.3.Використання сенсорних мереж в умовах сейсмоакустичного моніторингу при впливі ударної хвилі на об’єкти критичної інфраструктури

Сучасні загрози об’єктам критичної інфраструктури, зокрема промисловим, енергетичним, транспортним і військовим об’єктам, набувають нових форм у вигляді як природних, так і антропогенних факторів. Серед останніх найбільш небезпечними є впливи, пов’язані з ударною хвилею — результатом вибухів, надзвукових процесів або природних катастроф (землетрусів, техногенних викидів). Надійне виявлення та аналіз таких впливів вимагає застосування сенсорних мереж сейсмоакустичного моніторингу, що дозволяють в реальному часі оцінити ситуацію, визначити місце, потужність і напрямок дії джерела загрози, а також сформувати відповідну відповідь.

Сейсмоакустичний моніторинг — це метод отримання інформації про джерела механічних коливань у середовищі (грунт, повітря, вода) за допомогою реєстрації акустичних та сейсмічних хвиль. На відміну від класичних сейсмографічних систем, багатовузлові сенсорні мережі забезпечують більш

високу просторову роздільність даних, а також можливість адаптивного реагування на зміну динаміки зовнішніх факторів.

Сенсорні мережі «дають змогу здійснювати багатоточкову, синхронізовану реєстрацію сейсмоакустичних сигналів навіть у важкодоступних місцях», що є вирішальним для об’єктів критичної інфраструктури [31, с. 78].

Архітектура сенсорної мережі для сейсмоакустичного моніторингу

Типова структура сенсорної мережі, призначеної для моніторингу впливу ударної хвилі, включає такі основні компоненти:

1. Сенсорні вузли, що оснащені сейсмометрами, гідрофонами, акустичними мікрофонами, акселерометрами.
2. Комунікаційний рівень (зазвичай бездротовий, часто з використанням стандартів IEEE 802.15.4 або LPWAN).
3. Центральний вузол обробки (шлюз або сервер збору), що акумулює інформацію з усіх вузлів і здійснює її первинний аналіз.
4. Системи тривожного сповіщення та керування відповіддю.

Найбільш ефективною є кластерна організація мережі, в якій локальні вузли передають дані в центр кластера, а далі – до головного сервера. Слід зазначити, така архітектура «дозволяє підвищити стійкість мережі до часткових пошкоджень при дії вибухових хвиль та механічних вібрацій» [32, с. 112].

Сенсорні мережі, що працюють у сейсмоакустичному діапазоні, використовують різні типи сигналів — від інфразвукових до високочастотних, для:

-детекції моменту виникнення хвилі (зазвичай за різким зростанням амплітуди);

-визначення її напрямку поширення (за допомогою алгоритмів триангуляції);

-оцінки енергії або масштабу впливу;

-класифікації типу загрози (вибух, падіння конструкції, тектонічне зрушення тощо).

Завдяки синхронізації по GPS або локальному маяку, мережа дозволяє точно визначити часовий зсув сигналів і на його основі провести просторову локалізацію джерела.

Згідно з дослідженнями, точність локалізації при щільності розміщення вузлів 10 шт./км² сягає до 15 м, що є достатнім для реакції на загрози техногенного характеру [33, с. 45].

Переваги використання сенсорних мереж у таких умовах:

Масштабованість: можна швидко наростити кількість сенсорів у зоні ризику.

Самоорганізація: у разі втрати зв’язку між вузлами система автоматично перебудовує маршрути.

Низьке енергоспоживання: критично важливо для роботи в автономному режимі.

Гнучкість реагування: система може змінювати параметри фільтрації й чутливості на основі аналізу ризику.

Сенсорні мережі використовуються для моніторингу таких об'єктів:

Енергетичні станції (АЕС, ГЕС, ТЕС) – для виявлення підземних вибухів або змін геодинамічного середовища;

Мости, тунелі, дамби – контроль мікровібрацій, що можуть бути ознакою структурних порушень;

Військові об’єкти – аналіз вибухових хвиль від ворожих обстрілів;

Транспортні вузли – моніторинг навантажень і небезпечних впливів при аваріях.

Зібрана інформація з сенсорів обробляється з використанням методів:

цифрової фільтрації (наприклад, фільтри Калмана);

класифікації типів хвиль (швидкі/повільні, компресійні/поздовжні);

штучних нейронних мереж, які здатні виявляти патерни, характерні для певного виду впливу.

Впровадження системи на базі згорткової нейромережі дозволило досягти точності класифікації понад 96 % для ударних і сейсмічних подій [35, с. 87].

Попри значні успіхи, існують певні труднощі:

-обмежена енергоефективність при високій частоті дискретизації;

-складність розгортання в умовах відсутності зв’язку;

-вразливість до завад та навмисних атак на мережу;

-потреба у стандартизації протоколів обміну даними між сенсорами різного типу.

У майбутньому основну увагу буде приділено створенню самонавчальних, адаптивних сенсорних мереж, здатних самостійно калібруватись, змінювати архітектуру в разі пошкоджень і взаємодіяти з іншими типами розподілених систем безпеки.

2.4 Висновки до другого розділу

Інформаційна безпека сенсорних мереж в умовах зовнішніх загроз, у тому числі кібератак і навмисних електронних завад, є базовою складовою збереження функціональності таких систем у кризових ситуаціях. Напрямки її забезпечення охоплюють не лише традиційні криптографічні підходи, але й впровадження розподіленого контролю доступу, використання блокчейн-технологій, алгоритмів виявлення аномалій та самонавчальних нейронних мереж, здатних виявляти вторгнення без попередніх сигнатур. Комплексна реалізація зазначених заходів дозволяє забезпечити цілісність, конфіденційність та доступність даних навіть у режимі реального часу та за обмежених ресурсів.

У свою чергу, використання сенсорних мереж у сейсмоакустичному моніторингу в умовах дії ударної хвилі становить технологічно складне, але перспективне рішення для запобігання руйнівним наслідкам вибухових навантажень. Такі мережі забезпечують багатоточковий збір даних з високою просторовою роздільністю, виявлення місця та сили впливу з точністю до десятків метрів, а також ідентифікацію типу загрози на основі акустичних, сейсмічних та інфразвукових характеристик. Особливо важливим є те, що ці системи здатні функціонувати в автономному режимі та швидко адаптуватися до змін конфігурації середовища, зберігаючи стійкість навіть у разі часткового пошкодження компонентів мережі.

Важливо зазначити, що інтеграція таких сенсорних технологій у структуру об’єктів критичної інфраструктури дозволяє значно підвищити рівень їх

захищеності. Йдеться не лише про раннє виявлення загроз, а й про формування автоматизованої реакції — наприклад, запуск аварійних протоколів, перекриття аварійних каналів або ініціацію блокувань доступу. Сучасні реалізації таких рішень демонструють можливість створення інтелектуального захисного контуру, який здатен функціонувати незалежно від централізованих командних систем. У цьому контексті сенсорні мережі виступають не як допоміжна, а як ключова технологія у побудові стійких, самоадаптивних систем забезпечення безпеки національного рівня.

Таким чином, комплексне впровадження сенсорних мереж — із фокусом на захищеність, здатність до сейсмоакустичного моніторингу та підтримку функціонування об’єктів критичної інфраструктури — є необхідною умовою технологічної безпеки держави в умовах гібридних загроз. Висока ефективність, автономність і адаптивність цих систем дозволяють суттєво зменшити ризики як природного, так і техногенного походження, забезпечуючи сталу роботу важливих інфраструктур навіть у найбільш екстремальних умовах.

РОЗДІЛ 3. МЕТОД ПОБУДОВИ АДАПТИВНИХ СЕНСОРНИХ МЕРЕЖ В УМОВАХ КІБЕРВПЛИВУ

Сенсорні мережі є ключовими компонентами сучасних кіберфізичних систем, що забезпечують моніторинг та управління в реальному часі. Однак їхня ефективність та надійність значною мірою залежать від здатності виявляти та усувати несправності, які виконуються в процесі експлуатації. Одним із найбільш складних для діагностики типів несправностей є “блимаючі” відмови, які характеризуються нестабільною роботою вузлів та періодичними збоями у передачі або обробці даних.

Умови завадової обстановки, включаючи електромагнітні перешкоди, техногенні впливи та природні фактори, значно ускладнюють процес таких відмов. Додатковий виклик становлять кіберзагрози, які можуть імітувати або посилювати “блимаючі” відмови через атаки на вузли мережі, спотворення даних чи порушення протоколів передачі

Розробка перевірених методів діагностики таких несправностей є завданням для підвищення надійності та безпеки сенсорних мереж. Запропоновані рішення мають зменшити динамічний характер “блимаючих” відмов, адаптуватися до змінного середовища та забезпечити мінімальний вплив на продуктивність системи. Удосконалення методів діагностики дозволяє тимчасово виявити та локалізувати проблеми, забезпечуючи стабільну роботу мережі навіть у складних умовах експлуатації.

При проведені діагностування сенсорної мережі з “блимаючими” відмовами необхідно використовувати декілька рівнів. “Блимаюча” відмова –

це відмова, яка не виявляється візуально або одним із штатних методів й засобами контролю і або діагностики. Проте вказана відмова виявляється під час проведення штатного технічного обслуговування або при використанні спеціальних методів діагностування. На першому рівні виконуються прості діагностичні процедури, що використовують тестове діагностування, яке обписане в попередніх пунктах. Коли з їх допомогою вдається визначити сенсори, які відмовили, то на цьому діагностування буде завершене із найменшими витратами часу. В випадку неоднозначності визначення сенсорів мережі, які відмовили. Визначеному діагностичному сенсору необхідно запустити діагностичні методи, які здатні впоратися з складнішими відмовами. В основі такого підходу лежить припущення про те, що елементарніші відмови виникають набагато частіше, ніж складні. Тому не потрібно одразу використовувати потужні діагностичні процедури, що вимагають великих часових витрат.

В роботі отримано удосконалений метод діагностоування “блимаючих відмов” сенсорної мережі в умовах завадової обстановки та кібервпливу, який включає в себе два алгоритми, які утворюють дворівневу систему щодо діагностування сенсорної мережі із “блимаючими” відмовами. Розроблені алгоритми дозволяють здійснити діагностування із різною якістю та за різний час. У випадку коли відмови не вимагають дуже високої якості діагностування, то використовується перший алгоритм. Він простіший та швидший і дозволяє завершити діагностування з мінімальними часовими витратами. Якщо перший алгоритм не надає задовільної відповіді, то діагностування продовжується, проте, з використанням більш потужнішого другого алгоритму.

Нехай у нас дана сенсорна мережа, яка складається із $N \geq 2t+2$ сенсорів. Накладемо умову, що в даній мережі може відмовити не більше t сенсорів. Вказана модель дозволяє діагностувати більшу кількість відмов. Так зокрема, для сенсорної мережі, яка складається із $N=20$ сенсорів при відомій класичній моделі, яка містить $N \geq 3t+1$ сенсорів, кількість відмов не буде перевищувати

двох. Для моделі, яка запропонована цей показник дорівнює трьом. Для забезпечення властивості функціональної стійкості сенсорної мережі до t відмов запропонована модель вимагає меншої надмірності. Зокрема, для виявлення та ідентифікації двох сенсорів мережі, які відмовили $(t=2)$ у запропонованій моделі необхідно $N \geq 2t+2=18$ сенсорів, а у випадку класичної це число $N \geq 3t+1=19$, що є достатньо істотним.

Використаємо деякі припущення:

1) Запишимо зв'язки між сенсорами сенсорної мережі в вигляді повнозв'язного неорієнтованого графа. Тобто будь-яка пара сенсорів мережі може обмінюватися повідомленнями. Крім того кожен сенсор може визначити відправника повідомлення.

2) Система повинна бути синхронною. Синхронізація – це наявність механізму, що дозволяє всім сенсорам мережі одночасно перейти до методу діагностування. Іншими словами обробка та передача інформації, яка відбувається у сенсорній мережі може періодично уривається в деяких контрольних точках (КТ). Це можна робити, наприклад, використовуючи синхронізації годинників сенсорів під час ініціалізації мережі чи в подальші моменти експлуатації із використанням довільного методу взаємного інформаційного узгодження.

3) Сенсори повинні обмінюються інформацією, що вибираються із множини

$$Z=\left\{a, \overline{a}, \varnothing\right\},$$

де a – вид інформації, семантика якої змінюється в залежності від певного випадку; $\overline{a}$ – величина протилежна до a; $\varnothing$ – порожнє інформаційне повідомлення. Такий варіант інформаційного повідомлення використовується в тому випадку коли за вказаний період часу через даний канал зв'язку не надіслано жодного інформаційного повідомлення.

4) Кожний сенсор використовуючи методи діагностування може визначити стан $S(i)$. Визначений стан може приймати лише два значення FF (справний) та $FAIL$ (несправний).

5) У разі передачі сполучень із змінною семантикою процесор повинен витрачати на кожне інформаційне повідомлення час $DELAY(i)$. Даний час незалежить від того, якій кількості сенсорів дана повідомлення направляється.

6) Деякий сенсор i витрачає на отримання повідомлення від деякого сенсора j час, який запишемо у вигляді $DELAY\_MES(i,j)$.

7) Має місце нерівність:

$$DELAY(i) > (N-1)\ DELAY\_MES(i,j).$$

Припустимо, що сенсор k($k = 1,...,N$) є діагностичним сенсором. Вказаний сенсор k повинен передати інформаційне повідомлення кожному з інших сенсорів відповідно. Потім сенсори мережі обмінюються між собою повідомленнями щодо отриманої інформації від діагностичного сенсора. Одночасно кожен сенсор мережі складає початковий набір (ПН). За допомогою даного набору визначаються “нелояльні сенсори”. Наступним кроком визначаються ті, сенсори, які залишилися та досягають угоди щодо “наказу” діагностичного сенсора. Даний наказ можна представити у вигляді – “прийняти” чи “відкинути”.

Під поняттям нелояльності сенсора мережі мається наувазі здатність сенсора спотворити передавану інформації довільним чином. Зокрема, різні повідомленнях, які передає нелояльний сенсор передаються всім іншим доступним сенсорам мережі. У випадку коли діагностування сенсорної мережі допомагає кожному справному сенсору однозначно виявити несправні сенсори, то взаємна узгодженість між справними сенсорами та лояльним

діагностичним сенсором (якщо в мережі він є) буде отримана у випадку обробки кожним сенсором інформації тільки з лояльних сенсорів. Лояльність таких сенсорів визначається в результаті використання методу діагностування.

Нехай $a=0$, $\overline{a}=1$ і, пронумеруємо кожний сенсор в мережі номерами $n=1,2,3,...,N$. Даний номер повинен бути відомим всім сенсорам сенсорної мережі.

Базовий набір, який утворюється в n-му сенсорі, можна записати у вигляді матриці

$$A_n=\begin{bmatrix} a_{11}^n & a_{12}^n & a_{13}^n & \square & a_{1L}^n \\ a_{21}^n & a_{22}^n & a_{23}^n & \square & a_{2L}^n \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1}^n & a_{n2}^n & a_{n3}^n & \square & a_{nL}^n \\ \dots & \dots & \dots & \dots & \dots \\ a_{L1}^n & a_{L2}^n & a_{L3}^n & \square & a_{LL}^n \end{bmatrix},$$

де

$$L=2t+1;$$

в i-му рядку знаходяться значення інформаційних повідомлень всіх j-х сенсорів, які отримані в першому раунді i-м сенсором та передані даним сенсором в другому раунді в n-тий сенсор;

в j-му стовпці знаходиться значення інформаційних повідомлень одного і того ж j-го сенсора, які передані ним всім i-м сенсорам;

по головній діагоналі розміщені елементи a_{ij}^n, які є значеннями інформаційних повідомлень j-х сенсорів, що передані ними самим собі у першому раунді.

В алгоритмі будемо використовувати деяку функція $majority$, що можна означити по-різному. Надалі будемо використовувати наступне означення даної функції. Нехай дано вектор $e=\{e_i\}\ (i=1,2...,n)$ та розряди групуються на

основі використання ознаки рівності значень в групи $M_1, M_2, ..., M_m$, що не перетинаються. Очевидно, що $m \le n$.

Нехай $|M_1| > |M_2| > ... > |M_m|$, тут через $|M|$ позначено потужність множини M, а саме кількість елементів вказаної множини. Якщо розряди $\{e_i\}$, які містяться в M_1 мають значення v, то функція $majority$ можна визначити за допомогою рівності:

$$maj\{e_i\} = v.$$

Якщо $|M_1| = |M_2| = \cdots$, то значення функції $majority$ визначається знаходиться на основі вибору індексів групи із груп, що мають найбільший розміру.

Зауважимо, що в разі, коли $e_i = \{0, 1\}$ ($i = 1, 2, ..., n$) та отриманий вектор має парну кількість розрядів, то виконується нерівність $|M_1| > |M_2|$. В подальшому буде досліджено такий випадок векторів.

Нехай дана сенсорна мережа, яка складається з N сенсорів із номерами $1 \ldots N$. Перевірка в мережі виконується за рахунок взаємного обміну повідомленнями з припущеннях, що сенсорна мережа синхронна та про можливість сенсора, що одержує інформаційне повідомлення визначити сенсор, який її відправив.

Перший алгоритм удосконаленого методу діагностування включає в себе два етапи:

– етап пересилок інформаційних повідомлень (кроки 1-3);

– етап аналізу отриманих інформаційних повідомлень (кроки 4-7).

Другий етап виконується кожним сенсором в автономному режимі на основі інформаційних повідомлень, які ним були отримані на етапі пересилок.

Перший алгоритм можна представити у вигляді наступних кроків.

Крок 1. k-ий сенсор, що був вибраний на основі використання тестового діагностування назначається діагностичним сенсором. Діагностичний сенсор посилає іншим n-м сенсорам ($n \ne k$) повідомлення, позначимо його Z_k. Дане

повідомлення вибирається з множини $Z = \{a, \overline{a}, \varnothing\}$. Нехай для зручності номер k рівним $2t+2$.

Крок 2. Всі інші n сенсорів, обмінюються інформаційними повідомленнями, отриманими від k-го сенсора мережі на першому кроці. Зауважимо, що сенсори, в яких буде блимаюча відмова, передають суперечливі повідомлення іншим сенсорам.

Кожний n-й сенсор ($n = 1, ..., N-1;\ n \neq k$) утворює з отриманих повідомлень деякий вектор $STR(n)$, який містить $2t+1$ елементів, для розміщення інформаційних повідомлень, які він отриманих від всіх інших сенсорів, зокрема, і себе на даному кроці $STR(n) = (Z_1, Z_2, ..., Z_{N-1})$.

Крок 3. n сенсорів обмінюються векторами $STR(n)$ ($n = 1, ..., N-1$), із яких кожний сенсор утворює початковий набір в вигляді матриці A_n, де вектори $STR(n)$ ($n = 1, ..., N-1$) розміщені у вигляді рядків по зростанню номерів сенсорів (сенсорів, що посилають інформаційне повідомлення),. Згідно припущення один даний сенсор завжди можна визначити.

Крок 4. n-й сенсор, який використовує з функцію $majority$ по відношенню до стовпців матриці A_n, визначає по одному значенню даної функції для кожного стовпця, із котрих формує вектор PRS_n, елементи якого рівні

$$PRS_n(j) = majority\ \{a_{ij}^n \mid i = 1...N\}.$$

Крок 5. n-й сенсор визначає елементи власної матриці A_n a_{ij}^{n*} $i, j = 1...N-1$, що знаходяться на перетині стовпця j з рядком i, коли

$$PRS_n(j) \neq a_{ij}^{n*}. \qquad (4.1)$$

Загальне число зазначених елементів позначемо через $L_{\max}$. У випадку коли $L_{\max} = 0$, то переходимо до кроку 7.

Крок 6. n-й сенсор знаходить підозрювану область, яка задана логічним виразом

$$\sum \Pi = \bigwedge_{L=1}^{L_{\max}} (i_l \vee j_l), \tag{4.2}$$

де i, j– номери сенсорів мережі із елементів матриці a_{ij}^{n*}, які відповідають номеру рядка i та стовпця j елемента матриці A_n, який відрізняється від $PRS_n(j)$.

Далі співвідношення (4.2) перетворюється до диз'юнктивної нормальної форми. Для того щоб це виконати необхідно розкрити дужки та виконати перетворення. Іншими словами вираження із кон'юнкції перетворюється до вигляду диз'юнкції кон'юнкцій. Зокрема, для обліку обмеження (у не більше ніж в t несправних сенсорах) виключаються із розгляду ті терми ранг яких більше t, тобто з більш ніж t елементами. Надалі кожен з термів, які залишилися, визначає поєднання допустимих несправностей, що можуть призвести до всіх виявлених несправностей. Проте, це виконується за умови, що несправностей в мережі є не більше ніж t. Якщо у виразі $\sum \Pi$ залишається більше однієї терма, то результат діагностування буде неоднозначний тобто $DIAGNOZ = 1$, у протилежному випадку $DIAGNOZ = 0$.

Крок 7. n-ті сенсори утворюють матриці B_n, що отримані з матриць A_n за рахунок викреслювання рядків та стовпців, визначених сенсорів, номери котрих є в термах, які отримані після перетворень виразу $\sum \Pi$ на шостому кроці. Після формування B_n n-ті сенсори мережі визначають стан (справний чи ні) k-го сенсора використовуючи правило:

1) у випадку коли матриця B_n містить однакові елементи, то k-й сенсор справний тобто $DIAGNOZ = 0$;

2) у випадку коли матриця B_n містить різні елементи, то k-й сенсор несправний тобто $DIAGNOZ = 0$;

3) у випадку коли частина матриці B_n містить неоднакові елементи, а частина – однакові, то справність k-го сенсора не визначена тому $DIAGNOZ = 1$.

Крок 8. Кінець алгоритму.

Якщо алгоритм закінчився, а $DIAGNOZ = 1$, то діагностування проведене не успішно, а це слугує сигналом для діагностичного сенсора про нездатність *Першого алгоритму* провести діагностування. Якщо $DIAGNOZ = 0$, то *Перший алгоритм* справився з поставленою задачею, а діагностування виконано успішно.

Блок-схема *Першого алгоритму* представлена на рисунку 4.1.

Для доведення коректності *Першого алгоритму* запишемо наступні означення та теорему.

Означення. У випадку коли в матриці A_n сенсора n ($n = 1, ..., N-1$) є деякий помічений елемент a_{ij}^{n*} $(i \vee j)$ (на перетині рядка i із стовпцем j) ($i, j \in \{1,2,...,2t+1\}$, то вважатимемо, що сенсори i та j взаємно “оточують відносно несправності” один одного, а елемент a_{ij}^{n*} $(i \vee j)$ будемо називати елементом “оточених відносно несправності” сенсорів i та j.

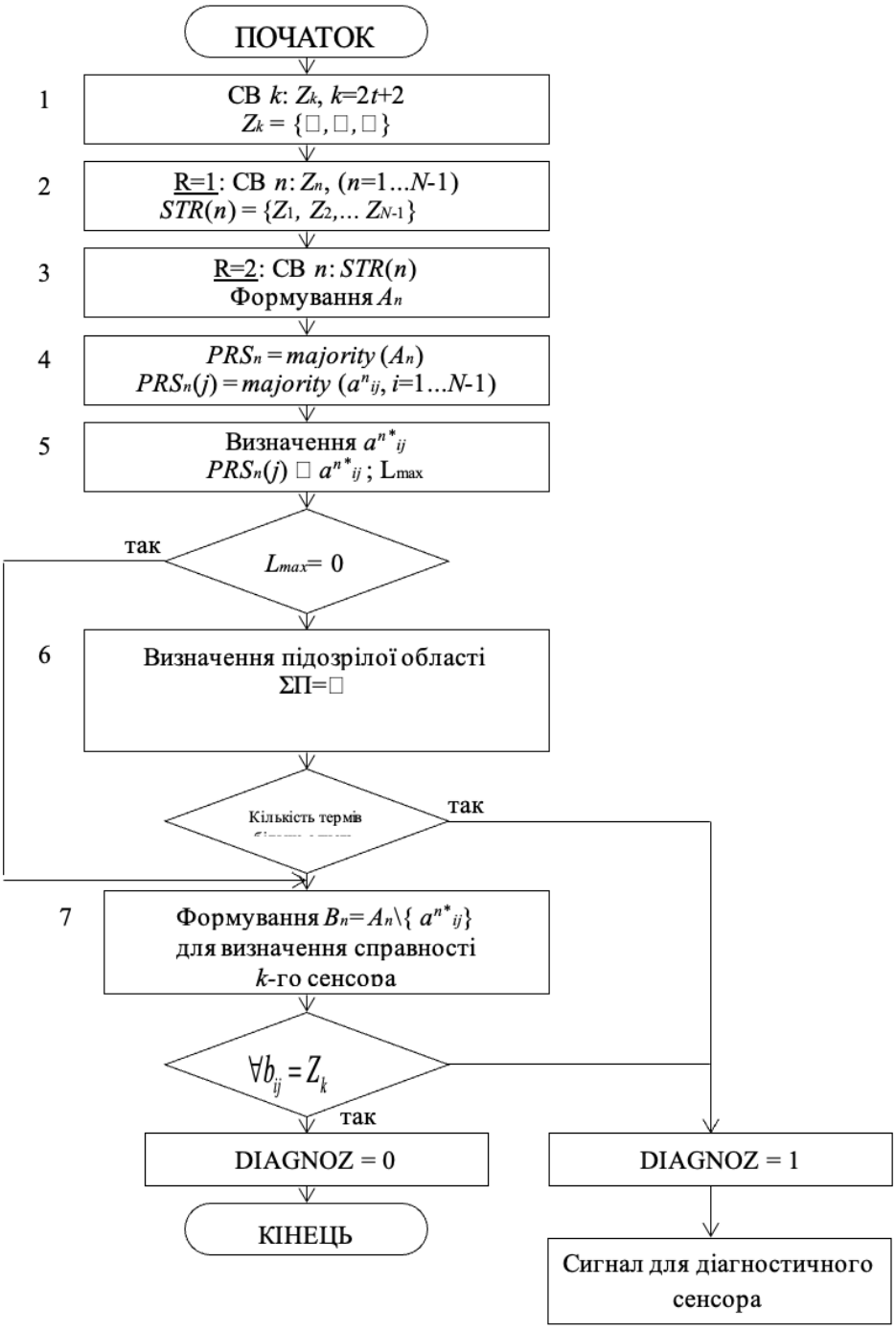

Рисунок 3.1 – Блок-схема Першого алгоритму удосконаленого методу діагностування

Означення. Сукупність всіх елементів “оточених відносно несправності” сенсора i для визначеної матриці A_n називатимемо “несправним оточенням” сенсора i та будемо позначати $ENVIR(i)_n$.

Теорема. У випадку коли для всіх справних сенсорів n сенсорної мережі, множина $S = \{S_1, S_2, ..., S_t\}$ несправних сенсорів, то між $\sum\Pi$ буде знаходитися правильне розв’язання $\overset{t}{\underset{i=1}{\wedge}} S_i$.

Доведення. Достатньо встановити, якщо сенсор n справний, то в його матриця суміжності A_n чи в рядку, чи в стовпці з номером $S_i \in S \ \ (i = 1 \ldots t)$ будуть в наявності помічені елементи з п’ятого кроку *Першого алгоритму*.

У випадку несправності S_i в мережі існує, два сенсори, які справні с з номерами p та m, такі, що S_i їм передаються різні інформаційні повідомлення впродовж другого кроку. Проте в силу своєї справності p та mпередають на третьому кроці сенсор n те, що вони получили від S_i на другому кроці без змін. Отже, $a^n_{mS_i} \neq a^n_{pS_i}$. Тобто після обробки власної матриці A_n сенсор n буде підозрювати S_i в несправності. Крім того, серед розв’язків буде присутнім і правильний розв’язок $\overset{t}{\underset{i=1}{\wedge}} S_i$.

У випадку коли несправність сенсора мережі проявилася лише на третьому кроці, то, можливо, правильний розв’язок не буде присутнім серед розв’язків всіх сенсорів. І це справедливо, тому що несправність сенсора не проявила себе у другому кроці, та не була поширена по всіх сенсорах за допомогою несправних сенсорів.

При даних припущеннях, удосконалений метод, який реалізується *Першим алгоритмом* призводить до наступного:

1. Коли в результаті самодіагностування сенсор n сенсорної мережі виявив свою несправність та в силі надати цю інформацію іншим сенсорам шляхом передачі інформаційного повідомлення $FAIL$ (в випадку комунікаційної

несправності також передано повідомлення $FAIL$, а це в силу семантичного позначення $\varnothing$), тоді *Перший алгоритм* вирішує завдання діагностування. Тут перший крок буде еквівалентним проведенню самодіагностування кожного сенсора мережі. Після третього кроку усі A_n включатимуть в собі вичерпну інформацію щодо діагностування сенсорної мережі: розряди PRS_n, які містять FF, відповідають справним сенсорам мережі, а ті, що містять $FAIL$ – несправним сенсорам сенсорної мережі.

2. Якщо в результаті виконання *Першого алгоритму* справний сенсор мережі отримує неоднозначний розв'язок задачі діагностування, то це буде свідчити про більше число сенсорів, які відмовили, чи про наявність складних "блимаючих відмов" із якими *Перший алгоритм* не в змозі впоратися.

Розглянемо деякі властивостей тестів.

Означення. Тести, що не містять програмних помилок будемо називати абсолютно надійними тобто поведінка яких однакова, незалежно від базових даних, для яких вони використовуються.

Означення. Тести називатимемо строго синхронними, якщо час обробки яких у кожному сенсорі буде відомий всім сенсорам мережі.

У випадку коли *Перший алгоритм* удосконаленого методу призводить до неєдиного розв'язання задачі діагностування, то діагностичний сенсор n переходить до використання іншого алгоритму, що дістав назву *Другий алгоритм*.

Другий алгоритм включає в себи декілька етапів. В свою чергу етапи можуть складатися з декілька фаз (див. рисунок 3.2). Обумовлюється існування механізму, що призначає на кожному етапі сенсор, який виконує діагностування. Такий сенсор і надалі будемо називати – діагностичним сенсором. Зауважимо, що під час етапу діагностичний сенсор не змінюється. *Другий алгоритм* регламентує дії діагностичного сенсора та дії сенсорів, які не є діагностичними сенсорами на кожному етапі.

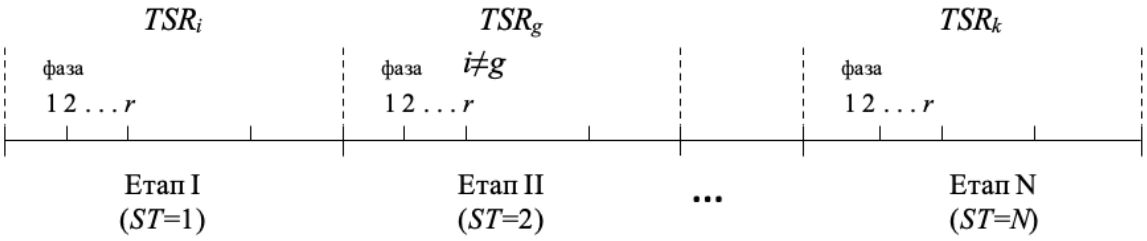

Рисунок 3.2 – Фази з часовою діаграмою

Довільна фаза певного етапу складається з наступних кроків:

Крок 1. Після прийняття рішення діагностичним сенсором сенсорної мережі щодо неспроможність *Першого алгоритму* тобто про його неоднозначну відповідь про стан сенсорів. Діагностичний сенсор TSR_i (i-й сенсор) посилає іншим j-м сенсорам $i \neq j$ інформаційне повідомлення, що в залежності від однозначності визначення стану СМ можуть бути записані у вигляді:

1а) “Я ВИЗНАЧИВ НЕСПРАВНІ СЕНСОРИ”. Таке інформаційне повідомлення посилається в разі, коли діагностичний сенсор у результаті виконання *Першого алгоритму* чи попередніх етапів чи фаз справного етапу *Другого алгоритму* визначив однозначно несправні сенсори мережі. Далі відбувається перехід до п.6.

1б) “ВИКОНАТИ ТЕСТ T_i^r”. У цьому випадку вказується заданий певним чином тест який потрібно виконати в фазі r. В даному випадку передбачається, що тести, сенсорів, які задаються, через сенсор i, вже доступні всім j-м сенсорам. Зауважимо, що в даній ситуації діагностичному сенсору (i-й сенсор) відомо, який час необхідно кожному з j-х сенсорів $i \neq j$ для опрацювання чергового тесту (нагадаємо, що тести повинні бути строго синхроними). Запишемо даний час як $t_T^r(j) = DELAY\ T_i^r(j)$.

Після закінчення часу $t_T^r(j) = DELAY\ T_i^r(j)$ i-й сенсор направляє j-му сенсору інформаційне повідомлення: «ВИКОНАТИ ТЕСТ T_i^{r+1}» і так далі.

Крок 2. Обмін даними між j-ми сенсорами $i \neq j$ про отримане завдання від i-го сенсора (діагностичного сенсора) виконати ТЕСТ T_i^r.

Крок 3. j-і сенсори мережі обробляють ТЕСТ $T_i^r(j)$.

Крок 4. j-і сенсори сенсорної мережі передають результати тестування $REZ\ T_i^r(j)$ i-у сенсору та повідомляють про ці результати один одному. При цьому, j-й сенсор, отримавши від k-го сенсора мережі результат тестування, повинен передати його номер k іншим l-м сенсорам ($l \neq k,\ l \neq j,\ l \neq i$), а повідомлення яке отримав діагностичному сенсору. Кожний j-й сенсор зберігає історію етапів (для кожного етапу ST матриця $G(r,n)$, де фіксується номер фази r певного етапу ST, номер сенсора n та момент отримання відповіді на тест від даного сенсора. Це продовжується до настання власного етапу. До початку якого обробляється вся історія попередніх етапів. Після закінчення власного етапу, продовжується запис історії етапів. Ця історія обробляється після закінчення всіх етапів, тобто після закінчення всього діагностування сенсорної мережі.

Крок 5. Діагностичний сенсор сенсорної мережі обробляє отримані повідомлення. Можливі випадки:

5а) Якщо протягом часу, що задається наступним чином

$$t^r(j) = t_T^r(j) + t_{\Pi}^r(i,j) =$$

$$= DELAY\,T_i^r(j) + (N-1)DELAY\_MES(i,j)$$

$t_T^r(j)$ – час, який витрачається j-м сенсором на опрацювання тесту T_i^r, що він отримав від діагностичного сенсора i в r-й фазі;

$t_{\Pi}^r(i,j)$ – час, який витрачається діагностичним сенсором i на отримання інформаційного повідомлення $MES(i,j)$ від j-го сенсора.

Діагностичний сенсор не отримає жодного повідомлення від j-го сенсора мережі, то прийняття рішення щодо стану такого “мовчазного” сенсора відкладається поки не завершаться всі етапи. У випадку коли після закінчення

останнього етапу стан j-го сенсора ще не визначений, то він вважається таким, що відмовив.

5б) Якщо протягом часу $t^r(j)$ діагностичний сенсор отримає повідомлення в вигляді:

$$\left\{REZ\ T_i^r(j),\ REZ\ T_i^r(j,l)\ |\ l \neq i,\ l \neq j\right\},$$

то потрібно перевірити наступне:

– чи правильні результати після виконання тесту

$$\left\{REZ\ T_i^r(j),\ REZ\ T_i^r(j,l)\ |\ l = 1...N,\ l \neq i,\ l \neq j\right\} = REZ\ T_{eman}^r;$$

– час вступу відповіді

$$t_T^r(j) = t_{emал}.$$

$REZ\ T_i^r(j)$ – результат обробки j-м сенсором тесту, який заданий у фазі r діагностичним сенсором i поточного етапу діагностування, а вираз $REZ\ T_i^r(j,l)$ – повідомлення про результати обробки l-ми сенсорами тесту, що заданий у фазі r діагностичним сенсором на поточному етапі діагностування, отримані j-м сенсором від l-х сенсорів у фазі r та передані діагностичному сенсору.

Зауважимо, що під час діагностування існують жорсткі часові обмеження, які визначені строго фіксованим часом опрацювання тесту та відомим часом, який витрачається щоб обробити кожне отримане інформаційне повідомлення.

У випадку коли результат обробки тесту буде неправильний чи час обробки не відповідає часовому ліміту, то сенсор буде вважаєтися таким, що відмовив та виключається з розгляду.

Крок 6. Після закінчення заданого числа фаз поточного етапу i-й сенсор, після незначної затримки, яка необхідної у випадку різної тривалості обробки тестів у різних сенсорах, передає повідомлення: «$МІЙ\ \ ЕТАП\ \ END$». Після цього визначається новий діагностичний сенсор етапу TSR_g (g-й діагностичний сенсор) $g \neq i$ та відбувається повторення кроків 1-6 алгоритму.

Кінець алгоритму.

Блок-схема *Другого алгоритму* представлена на рисунку 3.3.

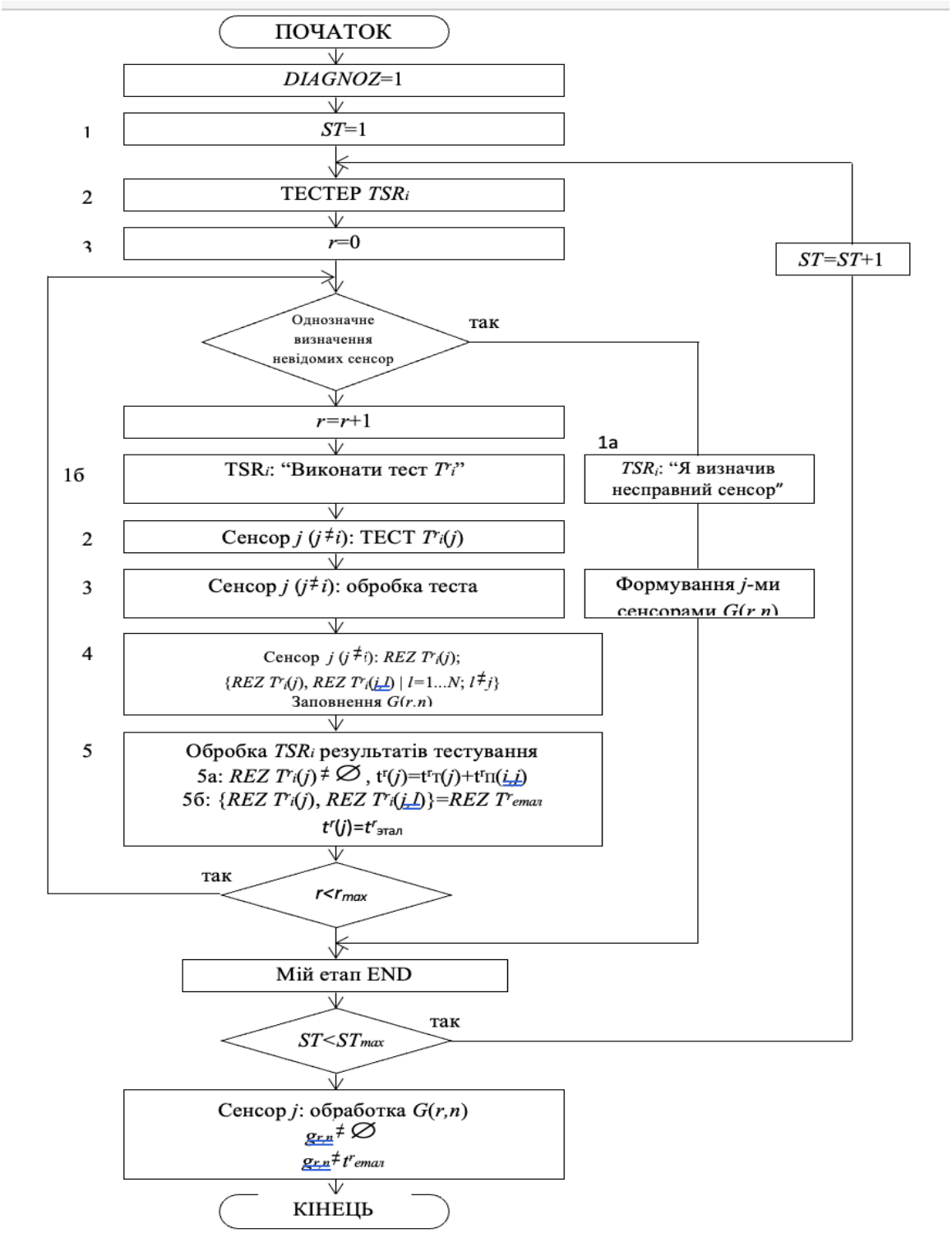

Рисунок 3.3 – Блок-схема Другого алгоритму удосконаленого методу діагностування

Необхідно зауважити, що i-й сенсор мережі може закінчити свій етап раніше. Він може не чекати завершення обробки всіх вказаних фаз на цьому етапі. Однак він це може зробити у випадку коли прийде до однозначного рішення завдання діагностування сенсорної мережі (крок 1а). в такому випадку по завершенню етапу виводиться повідомлення: “Я ВИЗНАЧИВ НЕСПРАВНІ СЕНСОРИ”.

Розглянемо коректність *Другого алгоритму* удосконаленого методу. Для початку зазначимо, що коли останньою фазою довільного етапу буде самодіагностування, то всі відмови, які знову проявлятимуться, будуть відомі у мережі. Якщо сенсор мережі має певну функціональну стійкість, то про виникнення відмов, із якими сенсор може самостійно впоратися, не буде повідомлятися іншим сенсорам. Отже, по завершенню кожного етапу нові відмови, які з'явилися впродовж даного етапу, будуть виявлені всіма справними сенсорами мережі. *Другий алгоритм* є коректним в тому випадку коли при виконанні припущень 5, 6 і 7 (які зазначені на початку пункту) сенсори з “блимаючими” відмовами будуть виявлятись кожним справним сенсором сенсорної мережі.

Розглянемо деякі випадки:

1. Якщо j-й сенсор несправний, то він передає суперечливу інформацію принаймні один раз упродовж всіх етапів діагностування. В противному випадку при виконанні *Другого алгоритму* відбудеться збій. Якщо несправний j-й сенсор проявився, то при опрацюванні наступного тесту, даний сенсор запізниться на $\Delta = t_T^r(j) - t_{T_{emal}}^r$ і це виявить діагностичний сенсор. Передача другого повідомлення у даній фазі буде записана в історії етапів тих сенсорів мережі, яким дане інформаційне повідомлення було направлене. А вже починаючи із наступної фази сенсор, який запізнився один раз, вже не зможе наздогнати втрачений час і він знову та знову буде запізнюватися тобто проявлятиме себе, як нелояльний.

Можливий і інший випадок – це передача неправильного результату поточного тесту. Тоді за рахунок неспівпадіння відповіді сенсора, який передав неправильний результат, він оголошується несправним.

2. Несправність j-го сенсора сенсорної мережі може проявлятись і в приховуванні інформаційних повідомлень, які отримані від справного сенсора. Проте в даному випадку буде з'являтися невідповідність між часом, який витрачено на отримання результату тесту T_i^r та обробку інформаційних повідомлень, що передаються діагностичному сенсору та лімітом часу що на це відводиться. Згідно із припущенням 6, якщо j-й сенсор посилає i-му сенсору інформаційне повідомлення, то i-й сенсор витрачає на його отримання деякий час $DELAY\_MES^r(i,j)$, тобто некоректний сенсор знову буде запізниться, а це дозволить всім іншим сенсорам виявити, що він несправний.

3. Найбільший інтерес викликає випадок, якщо сенсор "мовчить" тобто відправляє порожнє інформаційне повідомлення ($\varnothing$). Дане повідомлення не призводить до втрати часу, а це основне, що використовує *Другий алгоритм* та що відрізняє цей від *Першого алгоритму*. Якщо упродовж всіх етапів i-й сенсор мережі не отримав жодного інформаційного повідомлення від j-го сенсора, то по завершенню останнього етапу i-й сенсор робить висновок, що j-й сенсор несправній. Крім того, якщо j-й сенсор дійсно несправний, то ця інформація стала відомо всім, кому цей сенсор передавав свої інформаційні повідомлення (відповідно з припущенням 6 несправний сенсор буде спізнюватиметься з відповіддю, у випадку коли укриватиме, те що отримує інформаційні повідомлення від i-го. Або його несправність випливе при спробі передати іншим сенсорам суперечливі повідомлення).

У випадку коли j-й сенсор справний, але відсутній комунікаційний шлях, то отримаємо ситуацію, коли кожний з справних сенсорів мережі буде рахувати свого сусіда по вказаному комунікаційному шляху несправним. Будемо вважати, що дана ситуація допустима. Та її можна дозволити за рахунок

використання додаткових витрат часу, які дозволять визначити несправність вказаного комунікаційного шляху.

Тривалість *Другого алгоритму* можна визначити за допомогою наступної теореми.

Теорема. Якщо несправність j-го сенсора вперше проявилася під час обробки тесту T_i^r, то про несправність буде відомо всім справним сенсорам сенсорної мережі не пізніше, ніж в $(r+1)$-ій фазі етапу i.

Доведення. Розглянемо окремі можливі випадки прояву несправності в *j*-му сенсорі.

1) Можливість видачі більше ніж одного результату на тест T_i^r. Згідно з припущеннями 5 та 7, діагностичний сенсор мережі отримає інформаційне повідомлення щодо результату обробки тесту від j-го сенсора через час $t^r(j) > t^r_{Тетал}$ оскільки на j-й сенсор витрачено часу більше, ніж на отримання інформаційного повідомлень від всіх сенсорів та передачу одного результату про виконання тесту. Отже, в роботі j-го сенсора утворюється запізнення, що буде виявлено всіма сенсорам, що отримують інформаційне повідомлення щодо результати обробки тесту T_i^r j-м сенсором.

2) Замовчування щодо отримання будь-якого інформаційного повідомлення. Зрозуміло, що з'явиться невідповідність між часом витраченим фактично на передачу свого інформаційного повідомлення та отримання повідомлень від інших сенсорів та лімітом, що відводиться на передачу разового результату та на отримання певної кількості результатів, що вимагається в повідомленні даної фази. Кожний результат, про який замовчується, призводить до збільшення часу витраченого фактично на $DELAY\_MES^r(i,j)$. Дане запізнення з'явиться в $(r+1)$-ій фазі коли відбувається видача результату тесту даної фази та буде кратним $DELAY\_MES^r(i,j)$, а це і потрібно було довести.

Розроблені алгоритми дозволяють утворити дворівневу систему діагностування сенсорних мереж з “блимаючими” відмовами. *Другий алгоритм* допускає, що СМ можна зробити строго синхронною хоча б на час діагностування. Дана умова дозволить перевести “блимаючу” поведінку сенсора сенсорної мережі “В тимчасову область” та використати в ролі діагностичної ознаки швидкість проходження процесів в кожному з сенсорів мережі.

Питання про тести у *Другому алгоритмі* є принциповим. Якщо причиною “блимаючої” відмови будь-якого з сенсорів мережі буде апаратна несправність, то тести мають тестувати повністю апаратну частину кожного сенсора.

Отже, отримано два алгоритми, що утворюють дворівневу систему діагностування “блимаючих” відмов. Удосконалений метод діагностування починається з виконання *Першого алгоритму*. Перевагою якого, у порівнянні з відомими алгоритмами є те, що даний алгоритм вимагає меншої надмірності мережі. Він включає в себи лише два раунди обміну інформаційними повідомленнями між сенсорами мережі та забезпечує діагностування мережі у випадку відмови майже половини її сенсорів.

Якщо рішення діагностування на основі використання удосконаленого методу за рахунок *Першого алгоритму* отримується неоднозначне, то діагностичний сенсор запускає діагностування мережі на основі *Другого алгоритму*, що в ролі критерію використовує час виконання фаз даного алгоритму.

3.1 Висновки до третього розділу

Удосконалено метод діагностування відмов в сенсорній мережі за рахунок двох розроблених алгоритмів.

Розроблені алгоритми формують дворівневу систему діагностування сенсорних мереж із “блимаючими” відмовами. У другому алгоритмі передбачається, що сенсорну мережу можна зробити строго синхронною хоча б на період діагностики. Це дозволяє перевести “блимаючу” поведінку сенсорів у часову область і використовувати швидкість протікання процесів у кожному сенсорі як діагностичну ознаку.

Важливу роль у другому алгоритмі відіграють тести. У разі, якщо причиною “блимаючої” відмови є апаратна несправність одного із сенсорів, тести мають охоплювати перевірку всієї апаратної частини сенсора.

Таким чином, отримано два алгоритми, які утворюють дворівневу систему діагностування “блимаючих” відмов. Процес діагностування починається з виконання першого алгоритму. Його перевагою є знижені вимоги до надмірності мережі порівняно з іншими відомими підходами. Алгоритм обмежується двома раундами обміну інформаційними повідомленнями між сенсорами та забезпечує діагностування навіть у разі виходу з ладу майже половини вузлів мережі.

Якщо результат діагностики за першим алгоритмом є неоднозначним, діагностичний сенсор активує другий алгоритм. У цьому алгоритмі час виконання його фаз використовується як ключовий критерій для аналізу стану мережі та уточнення результатів діагностування.

ВИСНОВКИ

У результаті проведеного дослідження було вирішено актуальну наукову проблему, що полягає у створенні ефективної моделі та методів

самоорганізації безпроводових сенсорних мереж, здатних зберігати свою зв’язність і функціональність в умовах навмисних завад і кібервпливу. Запропоновано підхід, який базується на використанні тестового діагностування та забезпеченні відмовостійкої інформаційної взаємодії між вузлами мережі, що дозволяє своєчасно виявляти несправні сенсорні елементи й підтримувати стабільну роботу системи в умовах ускладненого середовища. Проведено комплексний аналіз сенсорних мереж із використанням мобільних агентів, у ході якого встановлено, що застосування стохастичних мобільних агентів у поєднанні з керованими марковськими процесами дозволяє істотно знизити енергоспоживання і продовжити життєвий цикл мережі завдяки оптимізованій маршрутизації. Також досліджено особливості дії навмисних завад у сенсорних мережах, які проявляються у вигляді цілеспрямованих атак, глушіння сигналу, спотворення інформації або фізичного впливу на вузли мережі. Встановлено, що такі завади істотно знижують ефективність функціонування мережі та можуть призводити до повної втрати зв’язку. Для підвищення стійкості мережі розроблено систему адаптивного захисту, що включає динамічне шифрування, зміну частотного діапазону, резервування критичних вузлів та впровадження систем виявлення аномалій у переданих даних. Крім того, удосконалено математичну модель діагностування сенсорної мережі шляхом введення матриці діагностичної інформації, яка формується за рахунок локальних перевірок між сусідніми вузлами. Здійснено перехід від централізованої моделі діагностики до розподіленої, у якій роль діагностичного центру виконує той вузол, який накопичує найбільший обсяг даних про працездатність інших елементів мережі. Такий підхід підвищує гнучкість системи, забезпечує її самодостатність у виявленні відмов і знижує залежність від зовнішнього контролю. Особливу увагу приділено проблемі так званих “блимаючих” або інтермітуючих відмов, які є складними для виявлення через їхню періодичну або випадкову природу. Для їх ідентифікації запропоновано дворівневу систему діагностування, яка на першому рівні

працює в умовах низької надмірності мережі та дозволяє локалізувати потенційно несправні вузли, тоді як другий рівень забезпечує уточнення діагностичних результатів через синхронізацію роботи вузлів і аналіз часових характеристик діагностичного процесу. Таким чином, у роботі обґрунтовано комплексний підхід до підвищення надійності та стійкості сенсорних мереж у складних умовах експлуатації, що поєднує енергоефективні методи маршрутизації, розподілені діагностичні алгоритми та механізми захисту від навмисних завад і кібератак. Запропоновані рішення можуть бути впроваджені в інформаційно-телекомунікаційні системи, зокрема в об’єктах критичної інфраструктури, системах безпеки, оборони, розвідки та в цивільних додатках, де потрібна висока надійність і автономність сенсорних мереж.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Гаврилюк І. С., Зінченко Р. О. Адаптивні методи маршрутизації у мобільних сенсорних мережах // Радіоелектроніка та інформатика. – 2022. – № 1.
2. Іващенко Н. Г. Географічні методи маршрутизації у WSN // Технології захисту інформації. – 2022.

3. Ігнатенко М. Військові сенсорні мережі: досвід Ізраїлю, США та НАТО // Воєнна аналітика. – 2021.
4. Коваленко Ю. В. Кластеризація сенсорних мереж з урахуванням енергетичного балансу вузлів // Збірник наукових праць ВІТІ. – 2020. – № 2.
5. Ковальчук І. Використання сенсорних систем у європейських арміях // Науковий вісник ХНУПС. – 2022. – № 1.
6. Кравець О. П. Архітектура безпроводових сенсорних мереж. – Львів : Видавництво ЛНУ, 2018.
7. Куценко В. С., Бондар Л. М. Моделювання маршрутів передачі даних у бездротових мережах // Збірник наукових праць Харківського університету Повітряних Сил. – 2021. – № 4.
8. Петренко І. М. Протоколи передачі даних у WSN : навч. посібник. – Київ : КНЕУ, 2020.
9. Покровський В. Розвиток бездротових сенсорних мереж у Збройних силах світу // Оборонна політика і безпека. – 2022. – № 2.
10. Романюк В. І. Сенсорні мережі : основи побудови та застосування. – Одеса : ОНПУ, 2021.
11. Семенов О. І. Протоколи маршрутизації у бездротових сенсорних мережах // Вісник НТУУ "КПІ". – 2021. – № 3 (75). –
12. Ситнік В. О. Основи побудови сенсорних мереж : навч. посіб. – Київ : НТУУ "КПІ", 2020.
13. Ткаченко М. С. Мультиагентні технології в безпроводових сенсорних мережах // Інформатика та кібернетика. – 2023. – № 3.
14. Шаповалов П. П. Аналіз показників якості каналу в задачах маршрутизації // Інформаційні системи та мережі. – 2021. – № 1.
15. Юрченко Т. Г. Оптимізація маршрутизації в безпроводових сенсорних мережах. – Харків : НТУ "ХПІ", 2019.

16. Воронін А. Сучасні технології сенсорного спостереження у військовій справі // Оборонний вісник. – 2021. – № 4. –
17. Баранник О. В. Основи побудови та захисту бездротових сенсорних мереж: навчальний посібник. – К.: НАУ, 2020. – 144 с.
18. Сидоренко А. В. Методи протидії активним завадам у бездротових сенсорних мережах // Системи обробки інформації. – 2021. – №3 (168).
19. Сіренко М. А., Каплій О. І. Безпека передачі даних у бездротових сенсорних мережах // Вісник НТУУ «КПІ». Серія: Радіотехніка. – 2020. – № 82.
20. Клименко Ю. А. Дослідження методів захисту інформації в бездротових мережах // Захист інформації. – 2022. – №1. –
21. Савченко І. О. Аналіз типів завад у сенсорних мережах та методів протидії // Радіоелектроніка, інформатика, управління. – 2023. – №2(57). –
22. Ільченко М. Ю., Марценюк І. М. Криптографічний захист у сенсорних мережах // Телекомунікаційні системи та технології. – 2021. – №4. –
23. Мельник А. І., Дьяків С. С. Адаптивні методи передачі інформації в умовах навмисного радіоперешкоджання // Системи управління, навігації та зв'язку. – 2022. – №3(67).
24. Демченко П. О. Штучний інтелект для виявлення завад у сенсорних мережах // Вісник ХНУРЕ. Серія: Радіоелектроніка. – 2023. – №1.
25. Рогозінський Д. Г. Протоколи маршрутизації в умовах деструктивного середовища // Вісник ЖДТУ. Серія: Технічні науки. – 2023. – №1(73).
26. Ященко І. О. Технології фізичного захисту інформації в розподілених мережах // *Вісник НАУ*. – 2022. – №3.
27. Степаненко Р. С. Еліптична криптографія у WSN: переваги та реалізація // *Радіоелектроніка та інформатика*. – 2022. – №2. –
28. Дмитренко А. О. Багаторівнева маршрутизація в сенсорних мережах із загрозами // *Системи управління та навігації*. – 2023. – №1.

29. Левченко К. В. Аномалієвий контроль сенсорних мереж на основі нейромереж // *Вісник КПІ*. – 2023.

30. Мельничук Т. І. Контроль доступу в інформаційно-телекомунікаційних системах // *Захист інформації*. – 2021. – №4.

31. Шмига П. М. Сенсорні системи в умовах моніторингу критичних об’єктів // *Технічні науки та технології*. – 2022. – №3.

32. Бойко В. Г. Архітектура бездротових мереж для сейсмічного моніторингу // *Збірник наукових праць ХАІ*. – 2021. – №6.

33. Михайлов М. І. Методи просторової локалізації джерел механічних коливань // *Інформаційні технології в безпеці*. – 2023. – №1.

34. Климович О. А. Використання сенсорних технологій у контролі технічного стану об'єктів енергетики // *Електроенергетика та контроль*. – 2021. – №2.

35. Савченко І. Ю. Ідентифікація акустичних подій у розподілених системах моніторингу з використанням ІІ // *Штучний інтелект і розпізнавання образів*. – 2023. – №4.