ПРОГРАМНО-ТЕХНІЧНІ КОМПЛЕКСИ

УДК 621.396

С.В. СКОРОБОГАТЬКО
Національний аерокосмічний університет ім. М.Є. Жуковського «Харківський авіаційний інститут», Харків, Україна, e-mail: *s.skorobogatko@csn.khai.edu*.

Г.В. ФЕСЕНКО
Національний аерокосмічний університет ім. М.Є. Жуковського «Харківський авіаційний інститут», Харків, Україна, e-mail: *h.fesenko@csn.khai.edu*.

В.С. ХАРЧЕНКО
Національний аерокосмічний університет ім. М.Є. Жуковського «Харківський авіаційний інститут», Харків, Україна, e-mail: *v.kharchenko@csn.khai.edu*.

С.В. ЯКОВЛЕВ
Національний аерокосмічний університет ім. М.Є. Жуковського «Харківський авіаційний інститут», Харків, Україна; Лодзинський політехнічний університет, Лодзь, Польща, e-mail: s*vsyak7@gmail.com*.

АРХІТЕКТУРА ТА МОДЕЛІ НАДІЙНОСТІ ГІБРИДНИХ СЕНСОРНИХ МЕРЕЖ СИСТЕМ ЕКОЛОГІЧНОГО ТА АВАРІЙНОГО МОНІТОРИНГУ

Анотація. Досліджено аспекти розроблення та аналізу працездатності гібридних сенсорних мереж як підсистем систем екологічного та аварійного моніторингу критичної інфраструктури. Запропоновано архітектуру гібридної сенсорної мережі, що ґрунтується на технології граничних обчислень (ГО) і поєднує стаціонарну і мобільну складові. Першу складову реалізують наземною сенсорною мережею (НСМ), другу — роєм безпілотних літальних апаратів, що утворюють летючу мережу ГО. Проаналізовано алгоритми збору даних, проблеми масштабування та оптимізації роботи НСМ і систем моніторингу в цілому. Розроблено та досліджено моделі надійності НСМ в умовах відмов одного та груп сенсорів. Отримано аналітичні залежності показників безвідмовності від різних за розмірами кластерів відмов сенсорів та їхньої інтенсивності. Надано рекомендації щодо проєктування та впровадження гібридних сенсорних мереж.

Ключові слова: гібридні сенсорні мережі, граничні обчислення, моделі надійності, множинні відмови, системи екологічного моніторингу, системи аварійного моніторингу.

ВСТУП

Системи екологічного та аварійного моніторингу відіграють ключову роль у гарантуванні безпеки довкілля та запобіганні негативним впливам на природу і людину. Їхня важливість зумовлена тим, що вони:

— дають змогу рано виявляти такі зміни в навколишньому середовищі, як забруднення повітря, води та ґрунту. Це створює умови для оперативного реагування на проблеми та вжиття заходів для їхнього усунення;

— дають можливість здійснювати контроль дотримання екологічних стандартів та нормативів об’єктами підвищеної небезпеки.

Основним компонентом систем моніторингу, який здійснює збір, передавання та аналіз різних видів даних, є сенсорна мережа. Сенсорні мережі підвищують ефективність систем моніторингу, роблячи їх більш точними, оперативними та економічно ефективними. Це зумовлено тим, що ці мережі:

— забезпечують широке охоплення території за рахунок розміщення великої кількості сенсорів у різних точках;

— сприяють оперативному реагуванню на надзвичайні ситуації техногенного та природного характеру завдяки можливості збирати та обробляти дані в режимі реального часу;

— дають можливість налаштовувати сенсорні вузли на вимірювання різних параметрів, що дає змогу створювати багатофункціональні системи моніторингу;

— зазвичай оснащені механізмами енергозаощадження, які гарантують довговічність роботи сенсорних мереж і зниження витрат на обслуговування;

— можуть працювати за бездротовими протоколами, що забезпечує гнучкість у розміщенні сенсорів та їхній мережевий зв'язок. Це особливо корисно в тих випадках, коли дротова інфраструктура може бути важкодоступною або дорогою;

— легко піддаються масштабуванню, що дає змогу додавати нові сенсори або розширювати покриття без значних змін в інфраструктурі.

Розвиток сучасних технологій відображається і в побудові сенсорних мереж. Зокрема набувають все більшої популярності гібридні сенсорні мережі, які використовують можливості граничних обчислень (edge computing) та безпілотних літальних апаратів (БпЛА). Сенсорні мережі в поєднанні з наземними і летючими сенсорами дають змогу створювати повніші й точніші моделі довкілля, що сприяє ефективному реагуванню на надзвичайні ситуації природного та техногенного характеру. Крім того, сенсорні дані можуть бути попередньо опрацьовані та відфільтровані бортовим комп'ютером БпЛА, що зменшує потребу в передаванні великих обсягів даних до наземного центру оброблення інформації, а отже, заощаджує пропускну здатність мережі та зменшує затримки.

Однак за межами досліджень багатьох науковців залишаються аспекти забезпечення надійності сенсорних мереж. Надійність є ключовим фактором для успішного функціонування та прийняття рішень у системах моніторингу. Надійна робота сенсорних мереж сприяє зниженню ризиків, зумовлених помилками в даних, а також підвищує ефективність систем моніторингу за рахунок скорочення часу простою і витрат ресурсів. До того ж надійні сенсорні мережі дають змогу скоротити витрати на технічне обслуговування і ремонт, оскільки знижується ймовірність їхніх відмов.

Метою статті є розроблення архітектури та моделей надійності гібридної сенсорної мережі систем екологічного та аварійного моніторингу з використанням граничних обчислень та БпЛА.

СУЧАСНИЙ СТАН ПРОБЛЕМИ

У роботі [1] розглянуто розроблення поверхонь ефективності, які характеризують взаємозв'язок між розміщенням сенсорів та ефективністю моніторингу. Запропонований алгоритм покращує моніторинг у приміщеннях шляхом оптимізації просторового розподілу сенсорних вузлів. Процес оптимізації враховує такі фактори, як оптимальне покриття, радіус дії та енергоефективність. У [2] запропоновано та досліджено бездротову сенсорну мережу на сонячних батареях для моніторингу параметрів навколишнього середовища. Використання цього альтернативного джерела енергії дає змогу подолати обмеження традиційних сенсорних мереж, зумовлені невеликим терміном служби звичайних батарей і потребою у їхньому доволі частому обслуговуванні. Автори [3] пропонують нову математичну модель, з використанням якої досліджено передавання пакетів між сенсорними вузлами та базовими станціями в межах бездротової сенсорної мережі (wireless sensor network, WSN). Модель враховує такі фактори як втрата пакетів, ретрансляція та механізми підтвердження. Нею можна скористатися для оцінювання впливу швидкості втрати пакетів, швидкості передавання та кількості спроб повторного передавання на загальну продуктивність доставки пакетів. У [4] розглянуто задачі оптимізації маршрутів для груп БпЛА, які інспектують та/або обслуговують визначені об'єкти з урахуванням альтернативних та динамічних баз (місць старту та/або посадки),

а також ресурсних обмежень. Запропоновані у цій статті математичні моделі та алгоритми оптимізації ґрунтуються на методах оптимізації мурашиних колоній, табу-пошуку та вичерпного пошуку. У роботі [5] основну увагу приділено плануванню логістичних місій для гібридних транспортних систем, що включають як наземну складову, представлену автомобілями або іншими транспортними засобами, так і повітряну (рій БпЛА), а також запропоновано математичні моделі, які ґрунтуються на алгоритмі оптимізації мурашиних колоній. Ці моделі дають змогу оптимізувати розподіл об'єктів за базами і генерувати маршрути БпЛА з урахуванням обмежень на ресурси польоту. Запропонована у [6] модель дає можливість систематично досліджувати важливі аспекти продуктивності мережі, а саме час безвідмовної роботи, час простою та вплив різних частот відмов сенсорів. Цю універсальну модель можна застосовувати до різних типів сенсорних мереж, включаючи бездротові сенсорні мережі та системи просторового моніторингу. У [7] автори представили результати комплексного дослідження моделей надійності сенсорних мереж. Під час моделювання використано метод Монте-Карло, баєсівські мережі та моделі простору станів. Модель, запропонована авторами [8], дає змогу прогнозувати та оцінювати надійність системи «Інтернет речей» (Internet of Things, IoT). Це дослідження сприяє розвитку методологій аналізу надійності систем на основі IoT і забезпечує підґрунтя для оцінювання та оптимізації продуктивності складних взаємопов'язаних мереж. У роботі [9] досліджено особливості функціонування архітектури летючих граничних обчислень, у якій БпЛА надають необхідні послуги користувачам в зонах природних катастроф з пошкодженою наземною інфраструктурою зв'язку. У ній також детально розглянуто поради щодо оптимізації кількості БпЛА та локацій їхнього розміщення з метою більш ефективного виконання граничних обчислень для користувачів. У [10] представлено архітектуру інтегрованої наземно-повітряної мобільної граничної мережі на основі БпЛА (названої авторами AG630 MEN). У цій мережі БпЛА виступають у ролі граничних мережевих контролерів, забезпечуючи ефективний розподіл обчислювальних ресурсів та ресурсів зберігання даних. Різні моделі надійності сенсорних мереж досліджено для розумних міст [11] з урахуванням варіантів резервування для стаціонарних [12] і мобільних [13] мереж, а також їхньої можливої деградації [14] та відновлення [15].

АРХІТЕКТУРА ГІБРИДНИХ СЕНСОРНИХ МЕРЕЖ

У цьому розділі представлено архітектуру сенсорної мережі з можливістю здійснення граничних обчислень та використання БпЛА для моніторингу об'єктів у реальному часі (далі — гібридна сенсорна мережа). Запропонована архітектура дає змогу виконувати збір, оброблення та аналіз даних моніторингу. Вона складається з трьох рівнів: хмарного рівня, рівня БпЛА і наземного рівня. Архітектуру гібридної сенсорної мережі можна адаптувати під сценарії застосування без рівня БпЛА за рахунок встановлення виключно наземного варіанта сенсорів і засобів збору/оброблення інформації. Ключовим компонентом представленої архітектури є хмарний рівень, який забезпечує зберігання даних, їхнє постоброблення, візуалізацію результатів та сповіщення про небезпеку. Хмарний рівень отримує дані, попередньо оброблені на нижчих рівнях (на рівні БпЛА та наземному рівні), та здійснює їхнє подальше оброблення й агрегування для отримання корисної інформації. Він також зберігає історичні дані, що дає можливість для глибокого аналізу, прогнозування майбутніх тенденцій та формування рішень.

Рівень БпЛА містить рій БпЛА, оснащених одноплатними комп'ютерами та сенсорами різного призначення, і забезпечує збір і первинне оброблення «сирих» даних моніторингу. БПлА рою можуть самостійно переміщуватися в контрольованому середовищі, виконуючи збір необхідних даних за допомогою бортових сенсорів і передаючи їх на наземний рівень для додаткового оброблення. Отже, БпЛА

забезпечують мобільність та гнучкість гібридної сенсорної мережі, здатної здійснювати моніторинг об’єктів на великих або важкодоступних територіях, де встановлення наземних сенсорів є неможливим або економічно неефективним.

Основний рівень формують пристрої, які можуть здійснювати граничні обчислення (далі — граничні пристрої). Їхня головна функція полягає у попередньому обробленні даних з мінімальною затримкою в межах ядра сенсорної мережі. Наземний рівень переробляє дані, отримані від рівня БПЛА, за допомогою алгоритмів машинного навчання чи інших аналітичних методів для добування інформації, важливої для подальшого прийняття рішень. Виконавши свою функцію, цей рівень відправляє оброблені ним дані до хмарного рівня для зберігання, додаткового оброблення та візуалізації. Наземні пристрої граничних обчислень дають змогу опрацьовувати інформацію безпосередньо в місці моніторингу, забезпечуючи своєчасне реагування системи та підвищення її загальної продуктивності. Приклад побудови архітектури наведено на рис. 1.

У тому разі, коли застосування у сенсорній мережі БпЛА є недоцільним, обговорювана архітектура може складатися з двох рівнів — наземного (сенсорів та граничних пристроїв у наземному виконанні) та хмарного. У такому варіанті архітектури граничні пристрої отримуватимуть дані від сенсорів, оброблятимуть їх та передаватимуть на хмарний рівень. Ця альтернативна конфігурація зберігає основні переваги граничних обчислень і може бути адаптована для великої кількості сценаріїв моніторингу об’єктів з використанням моделі доступності. Ця гнучкість дає змогу адаптувати систему відповідно до конкретних вимог або обмежень, забезпечуючи оптимальне використання ресурсів. Усунення рівня БпЛА (рис. 2) може сприяти зниженню витрат на впровадження архітектури та забезпечення її функціонування, при цьому зберігаються привабливі характеристики продуктивності та стабільності її роботи. Завдяки можливості масштабування гібридних сенсорних мереж та швидкості їхнього відгуку, ці мережі можна адаптувати відповідно до потреб кожного окремого прикладного завдання, яке виконує система моніторингу, до складу якої вони входять. Розви-

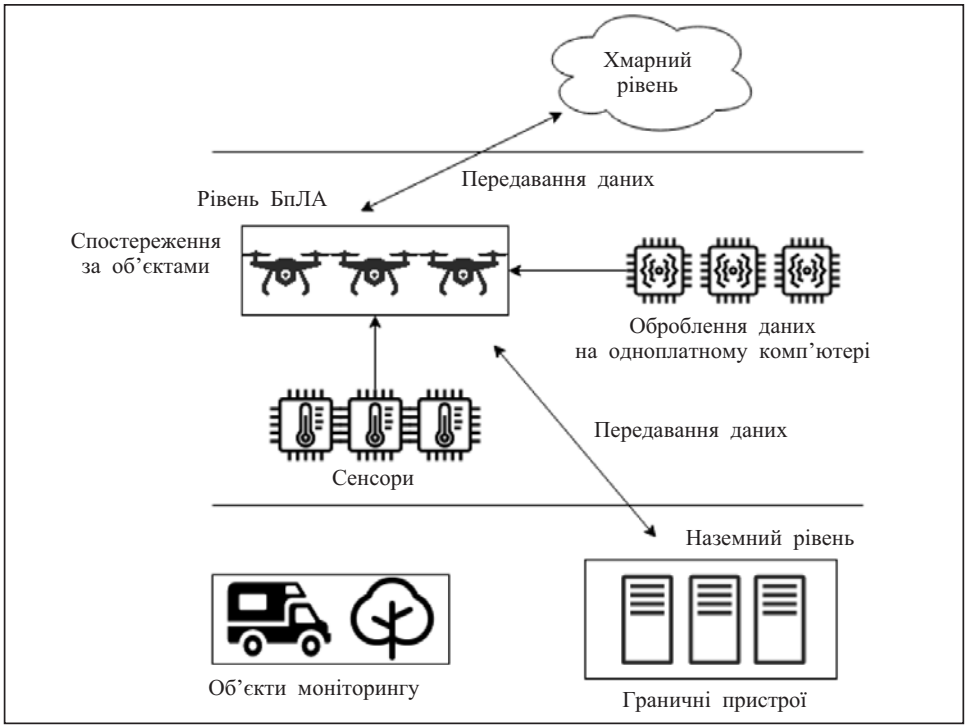

Рис. 1. Приклад трирівневої архітектури гібридної сенсорної мережі

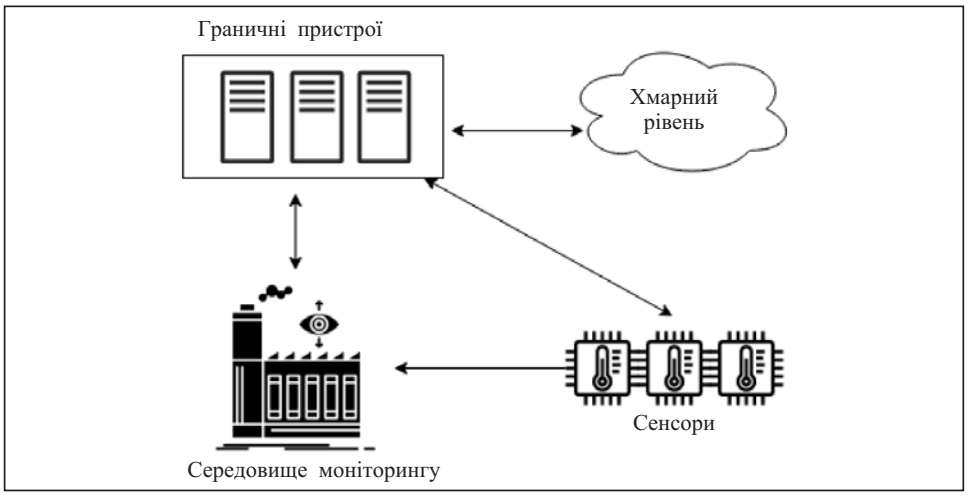

Рис. 2. Приклад архітектури гібридної сенсорної мережі без рівня БпЛА

ток сенсорних технологій та протоколів зв'язку також відіграє важливу роль у підвищенні надійності та безперебійності роботи всієї мережі.

МОДЕЛІ НАДІЙНОСТІ ГІБРИДНОЇ СЕНСОРНОЇ МЕРЕЖІ

Гібридні сенсорні мережі характеризуються самоорганізацією і здатністю адаптуватися до змін умов експлуатації, що забезпечує незначні витрати під час впровадження мережі та її подальшого супроводу. Однією з ключових переваг систем на основі сенсорних мереж є надійність мережі як цілісної системи — в разі збою одного з вузлів передавання даних здійснюється через сусідні елементи. Надійність мережі залежить від низки факторів: надійності апаратного та програмного забезпечення вузлів, території, де розгортають мережу, взаємного розташування вузлів, періоду регламентного обслуговування мережі, інтенсивності збору та передавання інформації кінцевими вузлами, розміру переданих пакетів інформації.

Класифікація моделей. Нижче наведено перелік моделей надійності сенсорних мереж, класифікованих за принципами конструювання та відновлення.

• Моделі безвідмовності нерезервованих сенсорних мереж без відновлення (МБ1). Це найпростіші моделі, які визначаються тільки кількістю та інтенсивністю відмов сенсорів і системного обладнання, а також визначенням критерію відмови мережі без урахування місць розміщення дефектних сенсорів мереж.

• Моделі безвідмовності сенсорних мереж, які враховують можливість резервування (дублювання) сенсорів (МБР2), коли кожен первинний сенсор резервується (дублюється) і резервний сенсор може замінити його в разі відмови.

• Моделі готовності нерезервованих і резервованих сенсорних мереж з відновленням (МГ1). Їхня відмінність полягає у тому, що вони враховують можливість відновлення дефектних сенсорів (наприклад, шляхом заміни).

• Моделі безвідмовності й готовності сенсорних мереж з можливістю врахування деградації систем моніторингу (часткової поступової втрати працездатності внаслідок відмов частини мережі або мережі в цілому за наявності резервних стаціонарних або мобільних мереж) (МГД2).

• Моделі безвідмовності і готовності сенсорних мереж з урахуванням розташування сенсорів (МБП3 і МГП3). Перелік цих моделей класифікують аналогічно описаним вище. В таких моделях критерій відмови може бути більш складним і визначатися не тільки кількістю, а й місцем розташування сенсорів, що відмовили.

Зауважимо, що частину означених моделей МБ1, МБР2, МГ1, МГД2 досліджено в [13–15], але не розглянуто моделі, які враховують просторове роз-

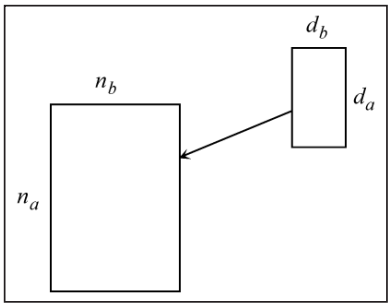

Рис. 3. Схема розташування груп сенсорів

ташування сенсорів, що відмовили.

Критерії відмови і показники безвідмовності. Критерій відмови сенсорної мережі визначається такими чинниками:

1) наявністю недопустимої кількості сенсорів, що відмовили (r), незалежно від їхнього розташування;

2) наявністю кластерної відмови визначеної кількості сенсорів, які розташовані поруч, що унеможливлює моніторинг на ділянці недопустимого розміру, яка має певну форму;

3) відмовою периферійного та системного обладнання мережі. В межах цієї роботи його безвідмовність не взято до уваги. Для того, щоб врахувати ці відмови, у межах консервативного підходу до оцінювання можна вважати, що будь-яка відмова цього обладнання призводить до відмови мережі.

Розроблення аналітичних моделей надійності сенсорних мереж. Для розроблення моделей припустимо, що ділянка моніторингу має форму прямокутника зі сторонами, які мають умовну довжину n_a і ширину n_b . Ці параметри збігаються з кількістю сенсорів, розміщених у рядках і стовпчиках ділянки. Отже, фізичні розміри ділянки моніторингу визначають як добуток її довжини n_a на ширину n_b. Тоді лінійка з n_b сенсорів повністю покриває відповідну смугу ділянки моніторингу, а матриця з n_a рядками і n_b стовпчиками повністю покриває всю ділянку.

Припустимо також, що критичними для функціонування мережі є кластерні відмови, яким відповідає ділянка прямокутної форми зі сторонами, що мають умовну довжину d_a і ширину d_b (рис. 3).

Зробимо узагальнення для груп суміжних сенсорів.

Розглянемо перший випадок, де

$$d_a \le n_a,\ d_b \le n_b,\ d_a < n_b,\ d_b < n_a,\ d_a \ne d_b.$$

Позначимо

$$L(n_a, n_b, d_a, d_b) = (n_a - d_a + 1)(n_b - d_b + 1) + (n_a - d_b + 1)(n_b - d_a + 1).$$

Ця функція визначає загальну кількість комбінацій, які є недопустимими з огляду на фіксовані розміри кластера відмов. Перший доданок описує кількість комбінацій покриття для вертикального розташування кластера відмов, другий — для його горизонтального розташування.

Тоді коефіцієнт структурної надійності сенсорної мережі, який визначається відношенням кількості її можливих працездатних станів за відсутності і наявності відмов сенсорів до загальної кількості можливих станів мережі, обчислюють за такою формулою:

$$K(n_a, n_b, r, d_a, d_b) = \frac{1}{2^{n_a n_b}} \left(\sum_{i=0}^{r-1} C^{\,i}_{n_a n_b} - L(n_a, n_b, d_a, d_b) \right). \qquad (1)$$

Тут у чисельнику зменшуване враховує першу складову критерію відмов і описує загальну кількість ситуацій з i відмовами в діапазоні від нуля до $r-1$, яка дорівнює кількості сполучень з $n_a n_b$ по i, а від'ємник визначає кількість недопустимих ситуацій з кластерними відмовами (друга складова критерію відмов).

Якщо сторони прямокутника для груп сенсорів є рівними $d_a = d_b = d$, то маємо

$$K(n_a, n_b, r, d_a, d_b) = \frac{1}{2^{n_a n_b}} \left(\sum_{i=0}^{r-1} C^{\,i}_{n_a n_b} - (n_a - d)(n_b - d) \right). \qquad (2)$$

Зауважимо, що отримані формули описують ситуацію, коли добуток величин d_a і d_b відрізняється від величини r на одиницю. По-перше, для загального випадку треба врахувати аспект парності і непарності цих чисел. По-друге, якщо різниця між добутком величин d_a і d_b та r перевищує одиницю, вираз для функції L буде визначатися сумою, кількість доданків якої залежатиме від цієї різниці.

Враховуючи модель для обчислення коефіцієнта структурної надійності, а також описані обмеження і припущення, отримаємо вираз для ймовірності безвідмовної роботи мережі. Ймовірність безвідмовної роботи сенсора $p(t)$ є функцією з експоненційним розподілом часу до відмови. Додатковим припущенням є те, що вплив зовнішніх факторів (фізичних впливів і можливих кібератак) на мережу не беремо до уваги.

Для розрахунків імовірності безвідмовної роботи мережі $P(n_a, n_b, r, d_a, d_b, t)$ враховуємо інтенсивність відмов сенсора. Отже, маємо:

$$P(n_a, n_b, r, d_a, d_b, t) = \sum_{i=0}^{r-1} C^{i}_{n_a n_b} (p(t))^{n_a n_b - i} (1 - p(t))^{i} -$$

$$- L(n_a, n_b, d_a, d_b)(p(t))^{n_a n_b - d_a d_b} (1 - p(t))^{d_a d_b}, \qquad (3)$$

де $p(t) = e^{-\lambda t}$.

Дослідження моделей надійності сенсорної мережі. Для моделювання функціонування сенсорної мережі вибрано лісовий масив у Малинівському лісництві Харківської області. У межах цього лісового масиву вибрано квадратну ділянку для розміщення однотипних сенсорів диму.

З використанням формули (3) складено табл. 1 та на її основі побудовано графіки залежності інтенсивності безвідмовної роботи сенсорної мережі від часу (рис. 4).

З аналізу табл. 1 та рис. 4 випливає, що:

— у разі застосування сенсорів з $\lambda = 1 \cdot 10^{-6}$ 1/год через 10000 годин функціонування сенсорної мережі її ймовірність безвідмовної роботи зменшиться відносно ймовірності безвідмовної роботи протягом 100 годин роботи лише у 1.01 раза, тоді як у разі застосування сенсорів з $\lambda = 1 \cdot 10^{-4}$ 1/год це зменшення становитиме 191.7 раза;

— заміна сенсорів з $\lambda = 1 \cdot 10^{-4}$ 1/год на сенсори з $\lambda = 1 \cdot 10^{-6}$ 1/год дає змогу збільшити ймовірність безвідмовної роботи сенсорної мережі для 5000 та 10000 годин роботи відповідно у 2.2 та 190.3 раза;

— у разі застосування сенсорів з $\lambda = 1 \cdot 10^{-4}$ 1/год вже через 5000 годин роботи ймовірність безвідмовної роботи сенсорної мережі зменшується у 2.2 раза, а через 10000 годин наближається до нуля.

Далі з використанням формули (3) отримано дані, представлені у табл. 2–4, та на їхній основі для різних значень ймовірності безвідмовної роботи сенсорів побудовано графіки залежності ймовірності безвідмовної роботи сенсорної мережі від недопустимої кількості сенсорів, що відмовили (рис. 5–7, на яких криву *1* побудовано для значень $n_a \cdot n_b = 64$, криву *2* — $n_a \cdot n_b = 81$, криву *3* — $n_a \cdot n_b = 100$, криву *4* — $n_a \cdot n_b = 121$, криву *5* — $n_a \cdot n_b = 144$).

Аналіз результатів розрахунків, наведених у табл. 2–4, та графіків, представлених на рис. 5–7, дає змогу зробити такі висновки:

— для всіх ділянок моніторингу збільшення недопустимої кількості сенсорів, що відмовили, призводить до збільшення ймовірності безвідмовної роботи сенсорної мережі. Наприклад для ділянки розміром $n_a \cdot n_b = 121$ збільшення

Таблиця 1. Ймовірність безвідмовної роботи сенсорної мережі для різних значень інтенсивності відмов сенсорів і часу роботи

Інтенсивність відмов сенсорів λ, 1/год	Час роботи сенсорної мережі t, год	Імовірність безвідмовної роботи сенсорної мережі як функція часу $P(t)$
$1 \cdot 10^{-4}$	100	0.999996
	1000	0.999948
	5000	0.451125
	10000	0.005217
	50000	$1 \cdot 10^{-29}$
$1 \cdot 10^{-5}$	100	0.999999
	1000	0.999996
	5000	0.999589
	10000	0.999948
	50000	0.451125
$1 \cdot 10^{-6}$	100	0.999996
	1000	0.99994
	5000	0.99992
	10000	0.99284
	50000	0.93899

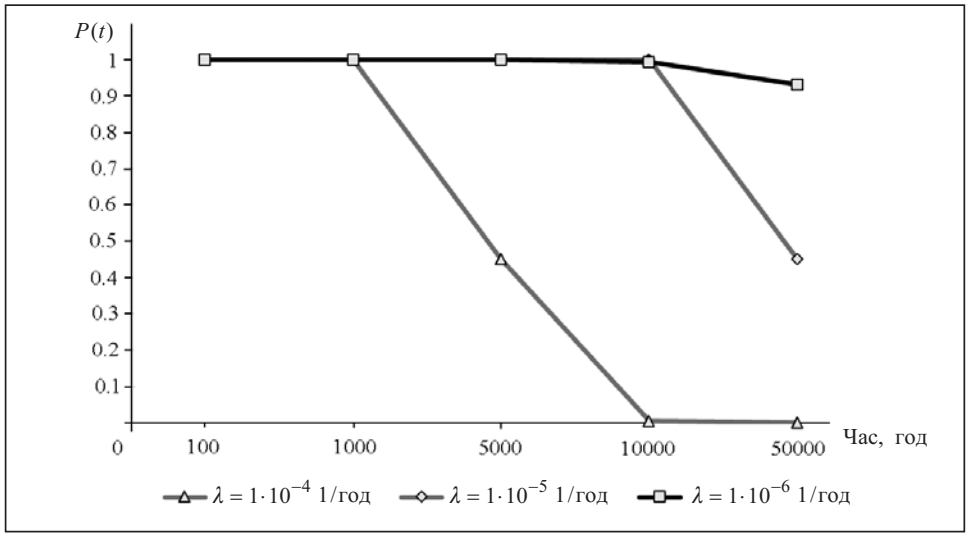

Рис. 4. Залежність імовірності безвідмовної роботи сенсорної мережі від часу для різних інтенсивностей відмов сенсорів ($r = 10$, $n_a = n_b = 5$, $d_a = d_b = 3$)

кількості таких сенсорів з 10 до 14 зумовлює зростання ймовірності безвідмовної роботи сенсорної мережі у 2.6, 1.3 та 1.1 раза для сенсорів з імовірностями безвідмовної роботи 0.85, 0.9 та 0.95 відповідно;

— за однакової недопустимої кількості сенсорів, що відмовили, менший розмір ділянки моніторингу забезпечує краще значення ймовірності безвідмовної роботи сенсорної мережі. Наприклад тоді, коли таких сенсорів 13, то для ділянки розміром $n_a \cdot n_b = 64$ ймовірність безвідмовної роботи сенсорної мережі буде у 2.6, 1.2 та 1.1 раза більшою, ніж для ділянки розміром $n_a \cdot n_b = 121$ у разі використання сенсорів з імовірностями безвідмовної роботи 0.85, 0.9 та 0.95 відповідно.

Таблиця 2. Ймовірність безвідмовної роботи сенсорної мережі для різних значень розміру ділянки покриття та недопустимої кількості сенсорів, що відмовили (для ймовірності безвідмовної роботи сенсора $p = 0.85$)

Розмір ділянки моніторингу, $n_a \cdot n_b$	**Недопустима кількість сенсорів, що відмовили, r**	**Ймовірність безвідмовної роботи сенсорної мережі як функція недопустимої кількості сенсорів, що відмовили, $P(r)$**
64	10	0.920191
	11	0.961859
	12	0.983372
	13	0.993365
	14	0.997569
81	10	0.760068
	11	0.854465
	12	0.918544
	13	0.957857
	14	0.979802
100	10	0.516381
	11	0.646493
	12	0.758453
	13	0.845784
	14	0.907957
121	10	0.274998
	11	0.391456
	12	0.515049
	13	0.634202
	14	0.739272
144	10	0.112111
	11	0.182934
	12	0.273671
	13	0.379437
	14	0.492384

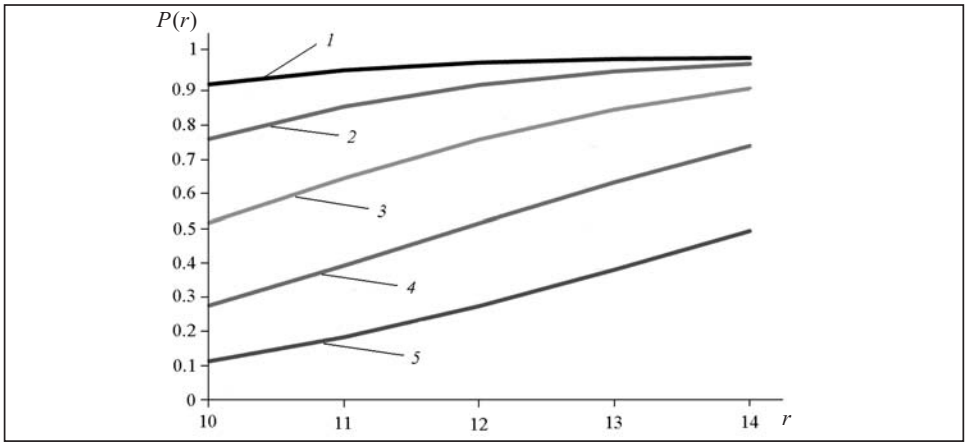

Рис. 5. Графік залежності ймовірності безвідмовної роботи сенсорної мережі від недопустимої кількості сенсорів, що відмовили, для різних розмірів ділянки моніторингу (для ймовірності відмови сенсора $p = 0.85$)

Таблиця 3. Ймовірність безвідмовної роботи сенсорної мережі для різних значень розміру ділянки моніторингу та недопустимої кількості сенсорів, що відмовили (для ймовірності безвідмовної роботи сенсора $p = 0.9$)

Розмір ділянки моніторингу, $n_a \cdot n_b$	Недопустима кількість сенсорів, що відмовили, r	Ймовірність безвідмовної роботи сенсорної мережі як функція недопустимої кількості сенсорів, що відмовили, $P(r)$
64	10	0.991966
	11	0.997377
	12	0.999224
	13	0.999791
	14	0.999948
81	10	0.962961
	11	0.984368
	12	0.993973
	13	0.997868
	14	0.999306
100	10	0.884655
	11	0.93967
	12	0.970962
	13	0.987096
	14	0.994689
121	10	0.737996
	11	0.836035
	12	0.90481
	13	0.948637
	14	0.974183
144	10	0.538526
	11	0.665276
	12	0.772616
	13	0.855321
	14	0.913701

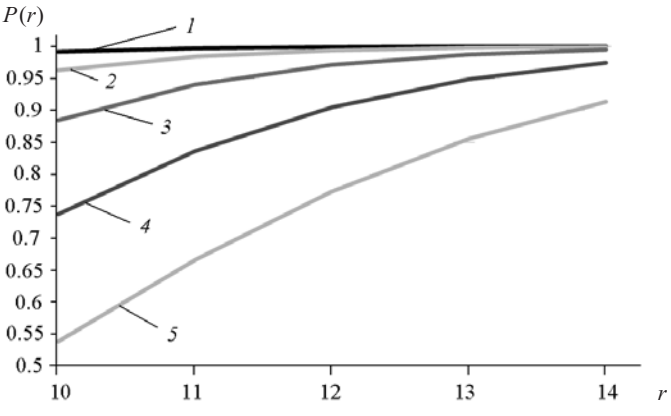

Рис. 6. Графік залежності ймовірності безвідмовної роботи сенсорної мережі від недопустимої кількості сенсорів, що відмовили, для різних розмірів ділянки покриття (для ймовірності відмови сенсора $p = 0.9$)

Таблиця 4. Ймовірність безвідмовної роботи сенсорної мережі для різних значень розміру ділянки моніторингу та недопустимої кількості сенсорів, що відмовили (для ймовірності безвідмовної роботи сенсора $p = 0.95$)

Розмір ділянки моніторингу, $n_a \cdot n_b$	Недопустима кількість сенсорів, що відмовили, r	Ймовірність безвідмовної роботи сенсорної мережі як функція недопустимої кількості сенсорів, що відмовили, $P(r)$
64	10	0.998763
	11	0.99969
	12	0.99993
	13	0.999986
	14	0.999997
81	10	0.992872
	11	0.997679
	12	0.999312
	13	0.999813
	14	0.999954
100	10	0.971812
	11	0.988528
	12	0.995726
	13	0.998536
	14	0.999537
121	10	0.917931
	11	0.959541
	12	0.98164
	13	0.992302
	14	0.997007
144	10	0.814658
	11	0.892233
	12	0.94197
	13	0.970983
	14	0.986488

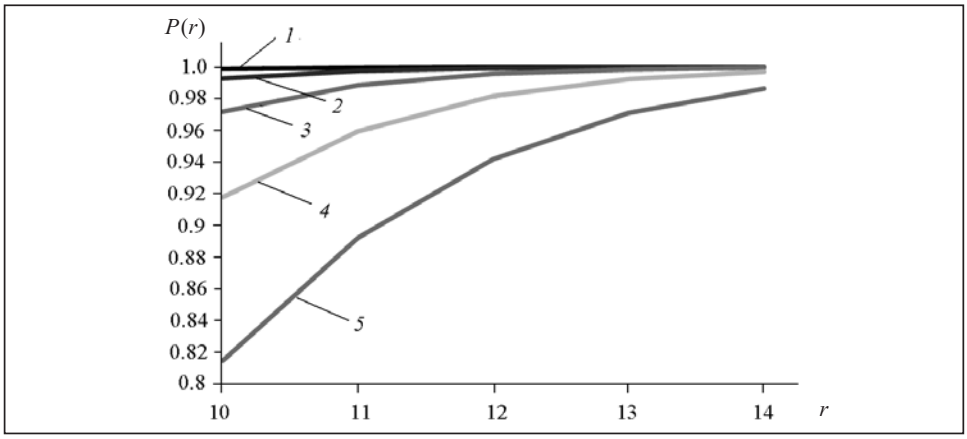

Рис. 7. Графік залежності ймовірності безвідмовної роботи сенсорної мережі від недопустимої кількості сенсорів, що відмовили, для різних розмірів ділянки моніторингу (для ймовірності відмови сенсора $p = 0.95$)

ВИСНОВКИ

Запропоновано архітектуру гібридної сенсорної мережі системи екологічного та аварійного моніторингу, що складається з трьох рівнів: наземного рівня, представленого наземними сенсорами та пристроями граничних обчислень; рівня БпЛА, оснащених бортовими сенсорами та одноплатними комп'ютерами;

хмарного рівня, який забезпечує зберігання даних моніторингу, їхнє постоброблення, візуалізацію результатів та сповіщення про небезпеку. Наведено приклад архітектури гібридної сенсорної мережі без рівня БпЛА.

Представлено перелік моделей надійності сенсорних мереж, класифікованих за принципами конструювання та відновлення. Цей перелік включає такі моделі: моделі безвідмовності нерезервованих сенсорних мереж без відновлення; моделі безвідмовності сенсорних мереж, які враховують можливість резервування (дублювання) сенсорів; моделі готовності нерезервованих і резервованих сенсорних мереж з відновленням; моделі безвідмовності і готовності сенсорних мереж з можливістю врахування деградації систем моніторингу; моделі безвідмовності і готовності сенсорних мереж з урахуванням розташування сенсорів.

Описано чинники, які визначають критерій відмови сенсорної мережі, та розроблено моделі надійності сенсорних мереж. З використанням розроблених моделей отримано залежності ймовірності безвідмовної роботи сенсорної мережі від:

— часу її роботи для різних інтенсивностей відмов сенсорів;

— недопустимої кількості сенсорів, що відмовили, для різних розмірів ділянок моніторингу та ймовірностей безвідмовної роботи сенсорів.

На підставі аналізу отриманих залежностей зроблено висновки про те, що:

— для всіх ділянок моніторингу збільшення недопустимої кількості сенсорів, що відмовили, зумовлює зростання ймовірності безвідмовної роботи сенсорної мережі;

— за однакової недопустимої кількості сенсорів, що відмовили, менший розмір ділянки моніторингу забезпечує краще значення ймовірності безвідмовної роботи сенсорної мережі.

Подальші дослідження автори планують спрямувати на розроблення імітаційних моделей надійності гібридних сенсорних мереж, що контролюють ділянки довільної форми та враховують різні недопустимі комбінації відмов сенсорів. При цьому підґрунтям для оптимального розташування датчиків з урахуванням зон їхньої дії та геометрії області моніторингу можуть слугувати моделі та методи розв’язування задач покриття, запропоновані в роботах [16–18].

СПИСОК ЛІТЕРАТУРИ

1. David P., Idasiak V., Kratz F. A sensor placement approach for the monitoring of indoor scenes. *Lecture Notes in Computer Science.* 2007. Vol. 4793. P. 110–125. https://doi.org/10.1007/978-3-540-75696-5_7.
2. Fasla K., Anil M. A solar energy harvesting system for WSN node in industrial sectors. *International Journal of Engineering Research & Technology (IJERT)*. 2022. Vol. 11, Iss. 6. P. 576–582. https://doi.org/10.17577/IJERTV11IS060270.
3. Zhou Y., Qian H., Wang Q., Li S. Performance modeling analysis of D-MSMR-CARQ with relay selection in wireless sensor networks. *Security and Communication Networks*. 2021. Vol. 2021. Article ID 5533926. 11 p. https://doi.org/10.1155/2021/5533926.
4. Horbulin V.P., Hulianytskyi L.F., Sergienko I.V. Optimization of UAV team routes in the presence of alternative and dynamic depots. *Cybernetics and Systems Analysis*. 2020. Vol. 56, N 2. P. 195–203. https://doi.org/10.1007/s10559-020-00235-8.
5. Horbulin V.P., Hulianytskyi L.F., Sergienko I.V. Planning of logistics missions of the “UAV+Vehicle” hybrid systems. *Cybernetics and Systems Analysis*. 2023. Vol. 59, N 5. P. 733–742. https://doi.org/10.1007/s10559-023-00609-8.
6. Arjannikov T., Diemert S., Ganti S., Lampman C. Using Markov chains to model sensor network reliability. *Proc. 2017 International Conference on Availability, Reliability and Security (ICARS)* (29 August – 01 September 2017, Reggio Calabria, Italy). Reggio Calabria, 2017. Article number 6. P. 1–10. https://doi.org/10.1145/3098954.3098979.
7. Chakraborty S., Goyal N.K., Mahapatra S., Soh S. A Monte-Carlo Markov chain approach for coverage-area reliability of mobile wireless sensor networks with multistate nodes. *Reliability Engineering and System Safety*. 2020. Vol. 193. Article number 106712. P. 1–14. https://doi.org/10.1016/j.ress.2019.106662.

8. Deif D., Gadallah Y. A comprehensive wireless sensor network reliability metric for critical Internet of Things applications. *EURASIP Journal on Wireless Communications and Networking*. 2017. Vol. 145. Article number 145. P. 1–18. https://doi.org/10.1186/s13638-017-0930-3.
9. Narang M., Xiang S., Liu W., Gutierrez J., Chiaraviglio L., Sathiaseelan A., Merwaday A. UAV-assisted edge infrastructure for challenged networks. *Proc. 2017 IEEE Conference on Computer Communications Workshops. INFOCOM WKSHPS'2017* (01–04 May 2017, Atlanta, GA, USA). Atlanta, 2017. P. 60–65. https://doi.org/10.1109/INFCOMW.2017.8116353.
10. Cheng N., Xu W., Shi W., Zhou Y., Lu N., Zhou H., Shen X. Air-ground integrated mobile edge networks: architecture, challenges, and opportunities. *IEEE Communications Magazine*. 2018. Vol. 56, Iss. 8. P. 26–32. https://doi.org/10.1109/MCOM.2018.1701092.
11. Catelani M., Ciani L., Bartolini A., Del Rio C., Guidi G., Patrizi G. Reliability analysis of wireless sensor network for smart farming applications. *Sensors*. 2021. Vol. 21, Iss. 22. Article number 7683. https://doi.org/10.3390/s21227683.
12. Akram V.K., Dagdeviren Z.A., Dagdeviren O., Challenger M. PINC: pickup non-critical node based *k*-connectivity restoration in wireless sensor networks. *Sensors*. 2021. Vol. 21, Iss.19. Article number 6418. https://doi.org/10.3390/s21196418.
13. Фесенко Г.В., Харченко В.С. Моделі надійності угруповань флотів БПЛА з ковзним резервуванням для моніторингу потенційно небезпечних об'єктів. *Радіоелектронні і комп'ютерні системи.* 2019. № 2 (90). С. 147–156. https://doi.org/10.32620/reks.2019.2.14.
14. Kolisnyk M., Kochkar D., Kharchenko V. Markov model of wireless sensor network availability. *International Journal of Computing*. 2020. Vol. 19, Iss. 3. P. 491–498. https://doi.org/10.47839/IJC.19.3.1899.
15. Fesenko H., Illiashenko O., Kharchenko V., Kliushnikov I., Morozova O., Sachenko A., Skorobohatko S. Flying sensor and edge network-based advanced air mobility systems: reliability analysis and applications for urban monitoring. *Drones*. 2023. Vol. 7, Iss. 7. Article number 409. https://doi.org/10.3390/drones7070409.
16. Yakovlev S.V. The concept of modeling packing and covering problems using modern computational geometry software. *Cybernetics and Systems Analysis*. 2023. Vol. 59, N 1. P. 108–119. https://doi.org/10.1007/s10559-023-00547-5.
17. Yakovlev S., Kartashov O., Podzeha D. Mathematical models and nonlinear optimization in continuous maximum coverage location problem. *Computation*. 2022. Vol. 10, Iss. 7. Article number 119. https://doi.org/10.3390/computation10070119.
18. Yakovlev S., Kartashov O., Mumrienko A. Formalization and solution of the maximum area coverage problem using Shapely library for territory monitoring, *Radioelectronic and Computer Systems*. 2022. N 2. P. 35–48. https://doi.org/10.32620/reks.2022.2.03.

S. Skorobohatko, H. Fesenko, V. Kharchenko, S. Yakovlev

ARCHITECTURE AND RELIABILITY MODELS OF HYBRID SENSOR NETWORKS FOR ENVIRONMENTAL AND EMERGENCY MONITORING SYSTEMS

Abstract. The authors study the aspects of developing and analyzing the hybrid sensor networks' operability as subsystems of environmental and emergency monitoring systems for critical infrastructure. The proposed architecture of such a system is based on the technology of edge computing (EC) and combines stationary and mobile components, the first of which is implemented by a ground sensor network (GSN), and the second by a swarm of unmanned aerial vehicles that form a flying EC network. The data collection algorithms, scaling problems, and optimization of the operation of the GSN and monitoring systems in general are analyzed. The reliability models of the GSN in the conditions of failure of one and groups of sensors are developed and investigated. Analytical dependencies of reliability indicators on different sizes of sensor failure clusters and their intensity are obtained. Recommendations for the design and implementation of hybrid sensor networks are given.

Keywords: hybrid sensor networks, edge computing, reliability models, multiple failures, environmental monitoring systems, emergency monitoring systems.

Надійшла до редакції 01.12.2023