DOI 10.31891/2307-5732-2024-331-16
УДК 621.391.8

МИХАЛЕВСЬКИЙ ДМИТРО
Вінницький національний технічний університет
http://orcid.org/0000-0001-5797-164X
e-mail: adotq@ukr.net
ШАПОВАЛОВА ТЕТЯНА
Харківський національний університет Повітряних Сил імені Івана Кожедуба
https://orcid.org/0009-0008-5467-7240
e-mail: jobs13qwer@gmail.com
СУХОТЕПЛИЙ ВЛАДИСЛАВ
Харківський національний університет Повітряних Сил імені Івана Кожедуба
https://orcid.org/0000-0002-2566-4167
e-mail: vladislav181168@gmail.com
ЛУЦЕНКО ОЛЕКСІЙ
Харківський національний університет Повітряних Сил імені Івана Кожедуба
https://orcid.org/0009-0000-2183-3130
e-mail: igmun1313@gmail.com

ПРОБЛЕМАТИКА ВИКОРИСТАННЯ БЕЗПРОВІДНИХ СЕНСОРНИХ МЕРЕЖ У ВІЙСЬКОВИХ ЦІЛЯХ

У статті проведено аналіз безпровідних сенсорних мереж для виявлення їх переваг та недоліків при використанні у військових цілях. Запропоновано розглядати архітектуру таких мереж на базі чотирирівневої моделі, яка складається із рівня сенсорів, рівня каналів передачі даних, рівня обробки даних та рівня додатків. Це створює універсальний і ефективний набір інструментів для вирішення різноманітних задач спеціального призначення для військових цілей. В такому випадку, кожен рівень може бути незалежним та характеризується відносною простотою та гнучкістю оперативного розгортання або оптимізації безпосередньо на лінії зіткнення.

Розглянуто особливості використання сенсорів для військових цілей, зокрема для вимірювання електромагнітних хвиль, світла, тиску, звуку, а також з урахуванням можливості створення сенсорних полів на базі безпілотних літальних апаратів та їх використання для забезпечення безпеки інформації. Проаналізовано особливості використання сенсорних мереж з урахуванням особливостей вибору сенсорів та оптимізації енергоспоживання для забезпечення ефективності та надійності системи.

Ключові слова: безпровідні сенсорні мережі, чотирирівнева модель, датчики, сенсорні поля, безпілотні літальні апарати, безпека інформації.

MYKHALEVSKIY DMYTRO
Vinnytsia National Technical University
SHAPOVALOVA TETIANA, SUKHOTEPLYI VLADISLAV, LUTSENKO OLEKSII
Ivan Kozhedub Kharkiv National University of the Air Force

PROBLEMS OF USING WIRELESS SENSOR NETWORKS FOR MILITARY PURPOSES

The article analyzes wireless sensor networks and identifies their advantages and disadvantages when used for military purposes. It is proposed to consider the architecture of the network based on a four-level model, which consists of the level of sensors, data channels, data processing and applications for creating various types of services. This creates a versatile and effective set of instruments for solving various tasks of special purpose for military purposes. The structure of a wireless sensor network for military use is considered in detail, taking into account the variety of sensors and their purpose. It also emphasizes the importance of compact and efficient sensors for military purposes, which contain means of digital information processing, receiver and transmitter, including measurements of electromagnetic waves, light, pressure, sound. The possibility of creating sensor fields based on unmanned aerial vehicles and their use for security and information gathering is noted. Data link parameters are detailed, including signal strength and signal level at the receiving end. The importance of space scanning radars for ensuring the safety of unmanned aerial vehicles in the conditions of wind speed and obstacles is noted. The article points out the problems of energy and computing resources when using sensors, in particular, the limitation of energy consumption and the length of the information transmission channel. Methods of rationalizing energy consumption by aggregating data and using clustering protocols are proposed. The main idea of the article is that the use of wireless sensor networks for military purposes requires attention to architectural details, sensor selection and power consumption optimization to ensure effective and reliable use of this system for its intended purpose, which will lead to the successful completion of the task by the unit. Therefore, the main advantages include the simplicity and flexibility of deploying sensor fields and the prompt receipt of information directly from the contact line, which is the key to a quick response to the enemy's actions.

Keywords: wireless sensor networks, four-level model, sensors, sensor fields, UAV, security and information gathering.

Вступ

Як відомо [1], широкого поширення отримали пристрої концепції IoT, які об’єднуються за допомогою телекомунікаційних мереж із використанням хмарних технологій для обміну та зберігання даних автономно без участі людини. Архітектура мереж IoT базується на використанні різного роду датчиків або сенсорів для відстеження та перетворення певних фізичних величин у інформаційні сигнали для подальшої обробки. Враховуючи широке поширення безпровідних технологій передачі інформації, в якості комунікації між пристроями, широкого поширення набули технології Wi-Fi, Bluetooth, Zigbee або системи масового обслуговування 4G/5G [2]. Таким чином, існує відносно простий і доступний механізм побудови систем збору інформації різноманітних процесів із подальшим аналізом та прийняттям рішень для широкого використання.

Аналіз останніх досліджень і публікацій та постановка проблеми

Одним із перспективних напрямків досліджень сенсорних мереж є їх застосування у військових цілях, що є особливо актуальним на даний час. Згідно з [3], під час проведення бойових дій, перевагу можна досягти за рахунок двох основних факторів: високий дух особового складу, націлений на перемогу в бою та всебічне технічне забезпечення бойових дій. Саме у сучасних умовах важливим фактором є необхідність мати перевагу у технічному забезпеченні та оперативному отриманні розвідувальної інформації безпосередньо із ліній зіткнення. Для цього, оптимальним застосуванням є безпровідні сенсорні мережі, які відіграють вирішальну роль у різних військових застосуваннях [4, 5], та дають ряд переваг: покращення спостереження, моніторинг різного роду параметрів і захист військ від загроз, операційна ефективність, зниження ризику, підвищення ефективності військових операцій та ін. Проте, враховуючи необхідність своєчасного забезпечення військ актуальною та достовірною інформацією, виникає ряд задач, до яких можна віднести [6, 7]: створення віддаленої мережі датчиків безпосередньо на лінії зіткнення, використання безпровідних каналів, необхідність адаптивного реагування на зміну параметрів зовнішнього середовища, завадостійкість, безпека, споживання енергії. Для пошуку нових рішень високоефективних сенсорних мереж, в першу чергу, необхідно виконати критичний аналіз використання безпровідних сенсорних мереж у військових цілях та визначити переваги та недоліки, що спричинені різного роду факторами впливу.

Метою роботи є аналіз безпровідних сенсорних мереж та виявлення їх переваг та недоліків при застосуванні у військових цілях.

Виклад основного матеріалу дослідження

Архітектуру сенсорних мереж можна охарактеризувати як чотирирівнева модель, що складається із: рівня сенсорів, для відстеження певних параметрів середовища; каналів передачі даних; рівня обробки даних; та рівня додатків для створення різного роду послуг. Враховуючи це, узагальнена структура сенсорної мережі для військових цілей можна представити як на рис. 1.

Базовою складовою сенсорних мереж є рівень сенсорів, що об'єднує різноманітні датчики у складі сенсорних вузлів, які здатні вимірювати різні фізичні величини [5]. Можливості та параметри датчиків визначають призначення та тип побудови мережі. Для військових цілей важливими фізичними явищами можуть бути: електромагнітні хвилі, світло, тиск і звук, які є результатом стрільби та вибухів. Тому, перевага надається датчикам, які можуть виявляти хімічні, біологічні та вибухові пари, а також присутність людей або предметів.

При побудові сенсорних мереж, можна окремо виділяти сукупність датчиків, для збору певного типу інформації, що можна об'єднати у так зване сенсорне поле. Такі поля можуть бути як автономними, підпорядковуватись безпосередньо до станцій наземного сегменту, або використовувати проміжні базові станції. Такі станції можуть бути стаціонарними або мобільними, наприклад, на основі БПЛА (безпілотних літальних апаратів) ретрансляторів, – так звана кластерна побудова. Крім того, існує можливість використання датчиків або створення цілого сенсорного поля безпосередньо на БПЛА. Приклад, процесу збору інформації із застосуванням сенсора та БПЛА наведено на рис. 2.

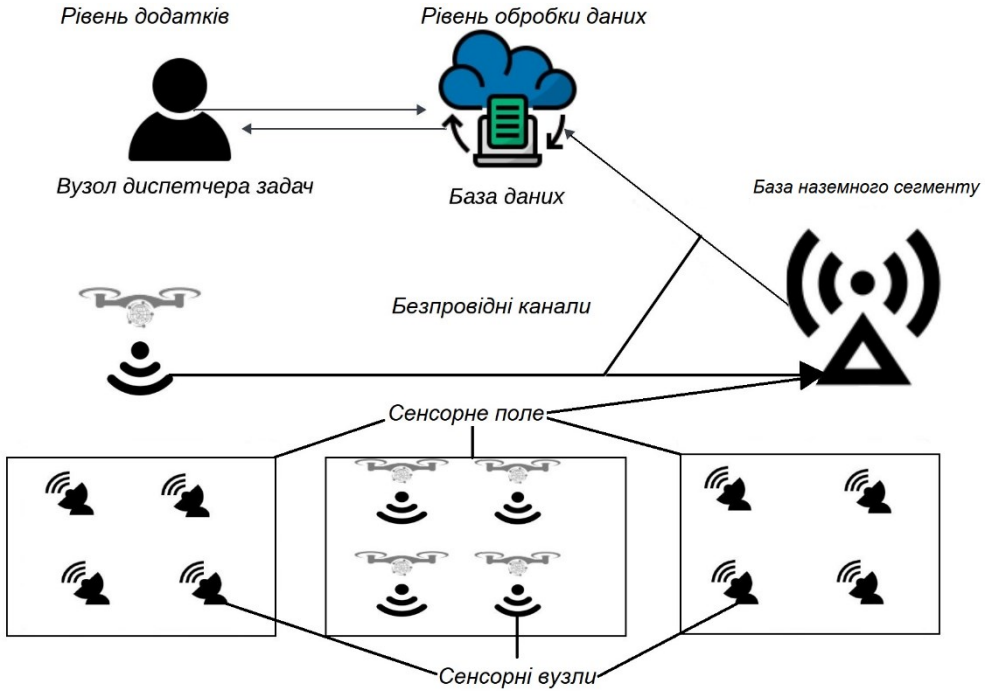

Рис. 1. Структура сенсорної мережі для військових цілей

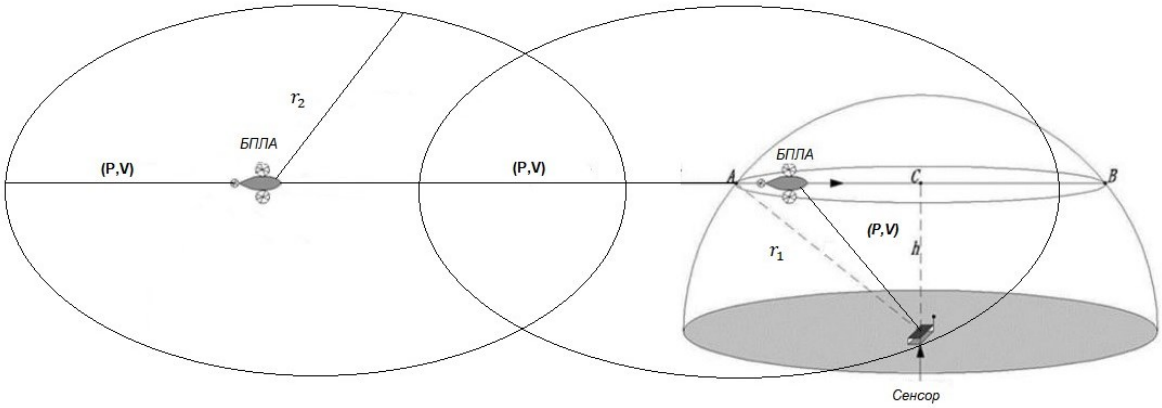

Рис. 2. Процес збору інформації БПЛА та сенсором

Сенсори, для військових цілей, мають компактні розміри і вміщують в собі засоби цифрової обробки інформації, приймач і передавач. Датчики забезпечують моніторинг об'єктів та контроль фізичних величин у певному радіусі дії на визначених ділянках. Сенсор після перетворення фізичної величини у цифровий код, обмінюється інформацією із базовою станцією на основі безпровідного каналу, що створений на базі пари приймач-передавач [7]. Канал характеризується наступними основними параметрами. Потужність сигналу передавачів сенсора та базової станції, що забезпечують зону покриття із радіусами r_1 і r_2 та відповідний рівень сигналу на приймальній частині P, щоб не було асиметричності. Таким чином, у зоні покриття (ABh) повинен існувати канал передачі інформації іх пропускною здатністю V [2] для забезпечення передачі кадрів без затримок до бази наземного сегменту.

Використання сенсорних полів на основі БПЛА висуває додаткові вимоги, оскільки виникає досить значна кількість додаткових факторів впливу, до яких можна віднести швидкість вітру та існування незначних перешкод з дерев та ліній електропередач. В такому випадку, використовують радари просторового сканування для забезпечення додаткових мір безпеки БПЛА.

Процес збору інформації за допомогою датчиків характеризується певними недоліками. що призводить до проблеми забезпечення живлення. В такому випадку, виникає обмеження на обчислювальні ресурси та довжину каналу передачі інформації. На лініях зіткнення, кожен датчик повинен працювати якомога довше, оскільки зарядка батареї може бути незручною або неможливою [8]. Сенсорний вузол повинен мати високі показники енергоефективності на рівні фізичного та канального рівнів, а також протоколів передачі даних та додатків прикладного рівня.

Якщо використовувати поділ сенсорної мережі на окремі сенсорні поля або кластери, то виникає велике навантаження на проміжні станції, де одним із методів зменшення енергоспоживання використовується агрегація даних на кожному проміжному вузлі [8]. Такий метод дозволяє значно простіше виконувати синхронізацію датчиків в межах одного сенсорного поля та підвищити можливості масштабованості й керованості мережі, за рахунок зменшення навантаження на проміжні вузли. Крім того, при такій організації можна значно оптимізувати трафік від базової станції виключенням однакових даних від сусідніх сенсорів. В свою чергу, агрегація додатково вносить свої затримки, що не є доцільним при отриманні оперативних даних для миттєвого реагування. Для зменшення такого недоліку застосовують протоколи HEED, LEACH і DESC. Як показують дослідження у [8] і [9], ефективність протоколів кластеризації також можна покращити за рахунок часткового об’єднання сенсорів у полі для зменшення кількості однотипної інформації та оцінюванням параметрів джерел живлення. За рахунок цього, в залежності від необхідної достовірності результатів отриманих даних, можна підвищувати автономність мереж у декілька разів.

Як відомо [3, 10], безпровідні сенсорні мережі використовують для моніторингу розташування противника, його кількість, характери дій, збір інформації про місцевість, використання в системах наведення інтелектуальних снарядів, вторгнення противника, забезпечення захисту підрозділів, оцінювання пошкоджень на полі бою, відстеження військових транспортних засобів, моніторингу державних кордонів та ін. Специфіка використання мереж на лініях зіткнення, передбачає існування загрози порушення функціонування, безпеки та компрометування інформації противником. Враховуючи специфіку сеансів передачі інформації у безпровідних каналах, можуть застосовуватись різні типи модуляцій сигналів із використанням хаотичних процесів. Такі процеси дозволяють маскувати радіосигнали у просторі формуючи у якості модулюючого коливання хаотичну послідовність. Додатково можна зазначити, що кластерна побудова робить мережу більш гнучкою, оскільки датчики у сенсорному полі зазвичай є однотипними, і відмова деяких із них не сильно вплине на параметри мережі.

Захист інформації у сенсорних мережах є більш серйозною проблемою у військових застосуваннях. Тут висуваються більш жорсткі вимоги до конфіденційності, цілісності, доступності та оперативності інформації. Порушення одного із цих параметрів може привести до критичних наслідків Згідно з [11] можна виділити наступні типи атак.

Атака Сивілли, це подія під час якої зловмисник бере контроль над вузлом певного кластера та підміняє данні отримані від сенсорів сенсорами, із можливістю створення уявних подій.

Атака на відмову в обслуговуванні – це намір зробити ресурси мережі недоступними, шляхом передачі радіосигналів однакових частот які використовуються сенсорною мережею або шляхом генерування великої кількості однакових повідомлень, що приведе до повторної передачі пакетів і збільшення трафіку.

Атака повторного відтворення передбачає додавання вузла із копіюванням ідентифікатора мережі. За допомогою такого вузла намагаються отримати криптографічні ключі та секретну інформацію.

Атака на сеанси передачі трафіку виконується при отриманні інформації про сегментний вузол мережі, що передбачає отримання пакетів, які надходять від різних вузлів сенсорів та подальший їх аналіз.

Атака прямої та зворотної секретності може бути проведена під час відмикання вузла від мережі під час різного роду збоїв, таких як помилка синхронізації, зменшення потужності випромінювання за рахунок енергозбереження та ін. Тоді під час повторного підмикання вузол буде виконувати попередній сеанс передачі кадрів який може бути перехоплений ворогом.

Фізична атака є основною загрозою на лініях зіткнення, яка передбачає остаточне знищення сенсорних вузлів.

Висновки

Отже, використання безпровідних сенсорних мереж для військових цілей дає універсальний і ефективний набір інструментів для вирішення різноманітних задач спеціального призначення. До головних переваг можна віднести відносну простоту та гнучкість розгортання сенсорних полів та оперативне отримання інформації безпосередньо із лінії зіткнення, що є запорукою швидкого реагування на дії противника.

Література

1. Mykhalevskiy D. Devising a technique to evaluate fluctuations in the main parameters of a wireless channel of the 802.11 standard. Easten-European Journal of Enterprise Technologies, No 6/9 (108), pp. 18–24. 2020. DOI: 10.15587/1729-4061.2020.218720.

2. Mykhalevskiy D. (2020). Development of a method for assessing the effective information transfer rate based on an empirical model of statistical relationship between basic parameters of the Standard 802.11 wireless channel. Eastern-European Journal of Enterprise Technologies, 5 (9 (107)), 26-35. doi: https://doi.org/10.15587/1729-4061.2020.213834

3. Mashtalir V., Zhuk O., Minenko L., Artyukh S. Conceptual approaches to the use of wireless sensor networks by the armies of advanced countries of the world. Modern information technologies in the field of security and defense. 2023. 47(2). p. 101–106.

4. Lee S. H., Lee S., Song H., Lee H. S. Wireless sensor network design for tactical military applications : Remote large-scale environments, Military Communications Conference, 2009. MILCOM 2009. IEEE. DOI: 10.1109/MILCOM.2009.5379900.

5. ðurišić M. P., Tafa Z. A Survey of Military Applications of Wireless Sensor. Mediterranean Conference on Embedded Computing. MECO – 2012. Bar, Montenegro. P. 1–4.

6. Jain U., Hussain M. Securing Wireless Sensors in Military Applications through Resilient Authentication Mechanism. Procedia Computer Science. Vol. 171, 2020, P. 719-728. Doi: 10.1016/j.procs.2020.04.078

7. Mikhalevsky D.V. Analysis of signal parameters in channels of the 802.11g standard for spectral problems. Proceedings of the international scientific and practical conference. "MSATPA" (October 20-22) 2014 Dubai. K.: Knowledge of Ukraine, 2014. p. 33–37.

8. Taheri H., Neamatollahi P., Yaghmaee M. H., Naghibzadeh M. A Local Cluster Head Election Algorithm inWireless Sensor Networks. 2011 CSI International Symposium on Computer Science and Software Engineering (CSSE) 15-16 June 2011. DOI: 10.1109/CSICSSE.2011.5963987.

9. Taheri H., Naghibzadeh M., Yaghmaee M. H. DESC: Distributed Energy Efficient Scheme to Cluster Wireless Sensor Networks. Wired/Wireless Internet Communications - 9th IFIP TC 6 International Conference, WWIC 2011, Vilanova i la Geltrú, Spain, June 15-17, 2011. DOI: 10.1007/978-3-642-21560-5_20

10. Ozerov S.V., Koval O.V., Kotyk Yu.O., Harvardt S.O., Marchenko E.V. Analysis of the possibility of applying chaotic processes to increase the secrecy of sensor networks of the tactical link of military command. Armament systems and military equipment. 2018. № 4(56). p. 42–45.

11. Jain U., Hussain M. Securing Wireless Sensors in Military Applications through Resilient Authentication Mechanism. Doi: 10.1016/j.procs.2020.04.078