ІННОВАЦІЙНІ ПРОЦЕСИ У ГАЛУЗЯХ АВІАЦІЇ, АВТОМОБІЛЕБУДУВАННЯ, РАДІОЕЛЕКТРОНІКИ, РАДІОТЕХНІКИ, ЗАСОБІВ ЗВ'ЯЗКУ ТА АСУ, А ТАКОЖ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

DOI 10.33099/2786-7714-2024-1-6-131-136

УДК 004.056

[1]**Опенько Павло Вікторович** **(кандидат технічних наук, старший дослідник)**
https://orcid.org/0000-0001-7777-5101
[2]**Довженко Надія Михайлівна** **(кандидат технічних наук, доцент)**
https://orcid.org/0000-0003-4164-0066
[1]**Оріховський Павло Володимирович**
https://orcid.org/0000-0003-4309-154X
[1]**Ікаєв Дмитро Русланович** **(доктор філософії)**
https://orcid.org/0000-0002-3501-0642

[1]***Національний університет оборони України, Київ, Україна***
[2]***Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна***

ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ ТА БЕЗПЕКИ У СУЧАСНИХ БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖАХ НА ОСНОВІ ВПРОВАДЖЕННЯ МЕТРИКИ RSSI

За останні десятиліття безпроводові сенсорні мережі (БСМ) зазнали значних трансформацій. Зокрема це стало можливим завдяки прогресу в технологіях, мініатюризації компонентів та зростанню потужності обчислень. Сенсорні мережі, як правило, складаються з великої кількості малопотужних багатофункціональних пристроїв, які розгортаються в певній географічній зоні. Хоч більшість з елементів такої мережі мають обмежені фізичні ресурси, об'єднані разом, вони швидко конфігуруються до виконання цілого ряду функціональних завдань у сфері науки, техніки, захисту критичної інфраструктури, захисту та моніторингу навколишнього середовища тощо.

Однак з розвитком та трансформацією БСМ все активніше досліджується й питання інформаційної безпеки, оскільки ризики несанкціонованого доступу або втручання можуть серйозно підірвати ефективність і надійність цих технологій. Доцільно зауважити, що саме через відкрите середовище передачі сигналів та інформації, необхідно покращувати, розвивати і впроваджувати оновлені й передові методи шифрування та автентифікації для забезпечення конфіденційності та цілісності даних. Крім того, критичного значення набуває розробка механізмів виявлення та реагування на атаки у сенсорних мережах. Все це потрібно для підтримки стабільності та безпеки як окремих сенсорних датчиків та вузлів, так і всієї мережі в цілому.

Ключові слова: *сенсорні мережі, безпроводові сенсорні мережі, інформаційна безпека, дані, безпілотний літальний апарат, надійність, вузли, датчики.*

Вступ

Переважно перспективність розвитку безпроводових сенсорних мереж (БСМ) базується на їх здатності адаптуватися до змін та вимог реального часу. Тому вони доброчинно впливають на розвиток в таких напрямках, як національна безпека, оборонні технології, автоматизація промисловості (Industrial Internet of Things, IIoT), безпілотні апарати (БПЛА), смарт-агрокультури, охорона здоров'я, "розумні" будинки та "розумні" міста.

Доцільно зауважити, що поступові кроки в інтеграції сенсорних мереж із БПЛА виражаються в їх здатності підсилювати наземні системи спостереження та моніторингу. Це поєднання надає нові можливості та підходи при виконанні складних, стратегічних завдань, покращує оперативність та ефективність реагування на кризові ситуації, шляхом збору, первинної обробки та передачі актуальних даних.

Наразі технології сенсорних мереж стають основою для глобальних інновацій, які змінюють спосіб ведення бойових (спеціальних) дій, бізнесу, управління екосистемами та підходи до особистісної безпеки.

Однак, використання потенційних переваг безпроводових сенсорних мереж вимагає високого рівня самоорганізації і координації між сенсорними датчиками для виконання завдань, необхідних для

підтримки основного призначення, а саме необхідність створення безпроводових сенсорних вузлів для самоорганізації в багатофункціональну мережу.

Створення інфраструктури сенсорної мережі для передачі даних вимагає встановлення безпечних зв'язків між довіреними сусідніми вузлами сенсорів [1], що набувають особливого значення під час застосування БСМ в зоні ведення бойових дій. Сам тому удосконалення підходів до забезпечення безпеки БСМ та інформації, що циркулює в таких мережах є важливим науковим завданням.

Аналіз літератури. Проведений аналіз існуючих наукових публікацій свідчить про наявність відповідних напрацювань у військовій сфері. Так, авторами [2] наведені тактико-технічні характеристики сенсорних систем спеціального (військового) призначення, особливості їх функціонування, узагальнено призначення мобільних БСМ оперативного рівня, а також розроблено рекомендації щодо впровадження таких систем у вітчизняній військовій сфері та їхнього подальшого інноваційного розвитку. В роботі [3] запропонована функціональна модель системи управління сенсорною мережею, обґрунтовано принципи побудови таких систем, їх структура та функції, розглянуті перспективи розвитку тактичних сенсорних мереж, наведена їх класифікація і вимоги, які висуваються до них. Авторами [4, 5] проведено аналіз безпеки мобільних радіомереж (англ. Mobile Ad-Hoc Networks (MANET)), визначені їхні основні вразливості, проведено класифікацію існуючих атак та оцінювання загроз, а також проаналізовано механізми забезпечення безпеки цих мереж. У роботі [6] запропоновано класифікацію атак у БСМ за чотирма ознаками, проте авторами не враховуються специфіка застосування БСМ у тактичній ланці управління військами. В [7] створено варіант програмно-апаратного комплексу, призначеного для просторово-часової інтеграції даних від засобів автоматичного наведення всіх підрозділів і пунктів управління частинами в рамках цифрової карти району бойових дій під управлінням частини під час бойових дій.

Таким чином, отримані результати в наведених роботах свідчать, що питанням забезпечення безпеки БСМ у воєнній сфері приділяється недостатня увага, а саме розгляд вразливості та атак стосовно БСМ виконуються в обмеженому обсязі, особливості їх функціонування та питання безпеки не враховується під час оцінки.

Мета статті. Удосконалення підходів до забезпечення безпеки безпроводових сенсорних мереж шляхом запровадження комплексного підходу, реалізація якого дозволяє запобігти зростаючим викликам і загрозам у цій області.

Матеріали та методи

У даному дослідженні застосовуються наукові методи системного аналізу та синтезу.

Результати

Для досягнення мети розглянемо покроково запропонований комплексний підхід.

Крок 1. Визначення загроз безпеці даних в сенсорних мережах

Оскільки БСМ часто розгортаються в неконтрольованих або незахищених фізичних умовах, важливо окремо приділити увагу впливу атак і загроз на вузли та сенсори. Виток інформації через фізичний доступ до вузлів може знищити цілісність і конфіденційність даних, що обробляються. Це ставить під загрозу не тільки окремі компоненти мережі, але й загальну безпеку системи в цілому.

У сенсорних мережах атаки можуть проводитися за різними сценаріями та на різних рівнях, зокрема у вигляді атак "jamming", спрямованих на внесення додаткових шумів та завад на фізичний канал передачі безпроводових сигналів. Також розглядається й фізичне втручання в роботу вузлів мережі, зокрема атака підміни сенсора, атака вилучення даних при прямому доступі зловмисника до складового елемента БСМ.

Коли розглядається вплив на канальний рівень, то частіше мова йде про атаки на створення колізій, якщо використовуються одні й тій же частотні канали, та атаки виснаження ресурсів вузлів мережі, в тому числі через примусову ретрансляцію пошкоджених пакетів вузлу-одержувачу.

На мережевому рівні зловмисники здійснюють шкідливий вплив на протоколи маршрутизації, включаючи підміну даних маршрутизації. Прикладом такої атаки є Black Hole атака. Ще одним прикладом атаки на мережевому рівні є атака типу Selective Forwarding. Передбачається здійснення вибіркових пересилань даних та пакетів компрометованим вузлом з ігноруванням решти запитів.

Крім DoS-атак, сенсорні мережі також вразливі до атак перехоплення та аналізу трафіку, що дозволяє зловмисникам отримати доступ до даних, здійснювати модифікацію та підміну їх для подальших атак на мережу й інші вузли. Тому необхідно використовувати відповідні методи шифрування та автентифікації для забезпечення конфіденційності і цілісності даних [8].

Крок 2. Стратегії протидії кібератакам на безпроводові сенсорні мережі

Управління ключами в БСМ є достатньо складним для реалізації завданням через значну кількість вузлів й, звісно, обмежені ресурси кожного з них. Розробка ефективних механізмів розподілу та оновлення ключів, які можуть адаптуватися до змін у топології та управлінню вузлами, є ключовим для підтримання безпеки в динамічних умовах.

Збільшення кількості сенсорів у мережі також створює проблеми з отриманням, первинною обробкою, зберіганням і передачею даних, оскільки традиційні методи можуть не справлятися з об'ємами даних, що постійно генеруються.

Використання технологій стиснення даних та розробка алгоритмів для вибіркової передачі

інформації може частково допомогти зменшити навантаження на мережу та оптимізувати її продуктивність. Однак в цьому випадку заходи щодо протидії атакам на безпроводові сенсорні мережі, вимагають більш жорстких кроків щодо комплексності зазначеного підходу.

Важливо не лише запровадити заходи захисту на кожному із рівнів, де виникає негативний вплив атак та загроз, але й забезпечити взаємодію захисних механізмів між собою. Наприклад, запровадження більш ефективного управління енергією та ресурсами на канальному рівні може своєю чергою допомогти мінімізувати вплив атак, які спрямовані саме на виснаження ресурсів.

Також корисним може бути впровадження розширених протоколів автентифікації та шифрування, що здатні зменшити ризики, пов'язані з атаками на фізичному та мережевому рівнях [9].

Використання нових підходів в методах шифрування, а також покращенні наявних алгоритмів безпеки на мережевому рівні може допомогти уникнути підміни даних маршрутизації та забезпечити додаткову цілісність і конфіденційність даних, тим самим успішно протидіяти атакам типу Black Hole і Selective Forwarding.

На транспортному рівні до атак на вузли сенсорних мереж належать Flooding-атаки, які спрямованні на виснаження ресурсів або пам'яті пристроїв, а також атаки, що здатні ввести перешкоди та порушення синхронізації, шляхом того, що зловмисники вносять помилки для перешкоджання коректній передачі даних легітимними вузлами.

Окрім базових цілей інформаційної безпеки, виражених у вигляді властивостей конфіденційності, цілісності, доступності та їхніх похідних, явно формулюються і вторинні цілі, які повинні враховуватися в процесі аналізу функціонування БСМ та її складових.

Зазначені цілі, зазвичай, формулюються для конкретної області застосування БСМ з урахуванням таких характеристик: актуальність даних, можливість самоорганізації мережі, синхронізація за часом, та безпека, що передбачає можливості відстеження вузлів та локалізації інцидентів інформаційної безпеки з визначенням конкретних елементів, які в них залучені.

Окрім цього, можуть враховуватися доступність вузлів мережі та даних, отриманих від них.

Таким чином, забезпечення безпеки БСМ реалізується шляхом застосування комплексного підходу, який включає захист від різноманітних типів атак, ефективне управління ресурсами і постійне оновлення безпекових механізмів, щоб відповідати зростаючим викликам і загрозам у цій області [10].

Крок 3. Визначення довірених вузлів у сенсорних мережах

Створення списків довірених, легальних вузлів у безпроводових сенсорних мережах, які можуть брати участь при передачі даних (логічній маршрутизації) є необхідним етапом для забезпечення надійності та безпеки мережі.

Для ініціалізації вузлів у безпроводових сенсорних мережах та визначення сусідніх вузлів, які знаходяться на відстані одного переходу (хопу) і при цьому являються довіреними, необхідно провести ряд розрахунків, а саме:

визначення досяжності сусідніх вузлів, що дасть інформацію про те, які вузли можуть безпосередньо комунікувати з даним вузлом без необхідності ретрансляції через інші;

проведення розрахунків показника сили сигналу RSSI (Received Signal Strength Indicator), який використовується для проведення оцінки відстані між вузлами. Відповідно, чим вищі значення RSSI, тим ближче знаходиться вузол, і тим ймовірніше він може бути використаний для хопу (передачі);

виявлення кількості довірених вузлів. Для підтвердження того, що сусідні вузли можуть бути довіреними, доцільно скористатися процедурою взаємної автентифікації за допомогою попередньо розділених ключів або цифрових сертифікатів;

визначення кількості доступних каналів, що сприятиме зменшенню колізій. Своєю чергою, це призведе до покращення розподілу трафіку в БСМ між вузлами;

визначення оптимальних параметрів для ретрансляції пакетів, які включають значення мінімальної енергії та оцінку навантаження на вузол.

Виявлення всіх сусідніх вузлів, які мають безпосереднє з'єднання з конкретним вузлом, можна здійснити через обмін пакетами по типу "hello", які включають інформацію про ідентифікацію та статус вузла [10].

Розрахунок значень RSSI для визначення відстані до сусідніх вузлів може бути реалізований наступним чином:

$$d = 10^{\frac{P_t - RSSI - L}{10n}}, \qquad (1)$$

де d – відстань між вузлами, P_t – вихідна потужність сигналу передавача, $RSSI$ – індикатор сили прийнятого сигналу, L – константа зсуву (залежить від конкретних умов середовища), n – коефіцієнт затухання сигналу.

Значення n зазвичай коливається між 2 і 4, а значення константи зсуву залежить від конкретних умов середовища, де розгортається сегмент БСМ.

При проведені розрахунків можна визначити, по-перше, на якій відстані знаходиться кожен сусідній вузол від конкретного елемента сенсорної мережі; по-друге, можна визначити, чи доцільно вузлам призначати статус "сусідній вузол на один хоп".

Оскільки RSSI і відстань мають неоднозначну залежність і можуть змінюватися залежно від конкретного середовища впровадження, тому для спрощення припускається, що вузли можуть передавати інформацію та "спілкуватися", якщо вони знаходяться на відстані меншій за заданий радіус зв'язку.

Рис. 1. демонструє базову топологію мережі, де вузли з'єднані між собою залежно від їхнього сигнального радіусу.

Маємо модель сенсорної мережі, яка створена з 10 вузлами, розташованими випадковим чином. Кожен вузол має зв'язок з іншими вузлами у межах певного радіуса. Після цього, визначено які з вузлів можна вважати довіреними.

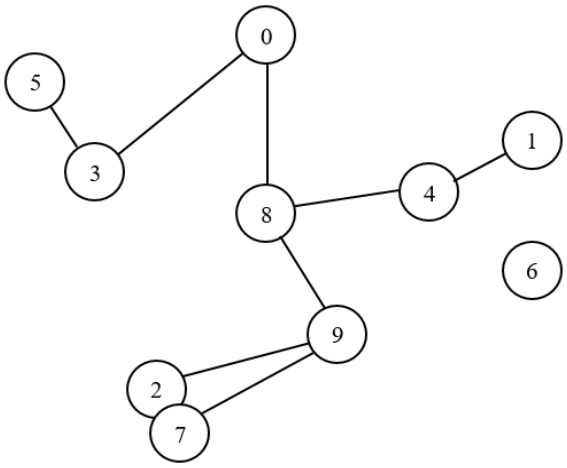

Рисунок 1. Приклад зв'язності у безпроводовій сенсорній мережі

Після проведення розрахунків довірених вузлів, можна припустити, що вузли перевіряються на довіреність на підставі їхніх ресурсів, таких як обчислювальна потужність та енергетичні запаси, які визначено випадково.

Довірені вузли позначені іншим кольором (рис. 2).

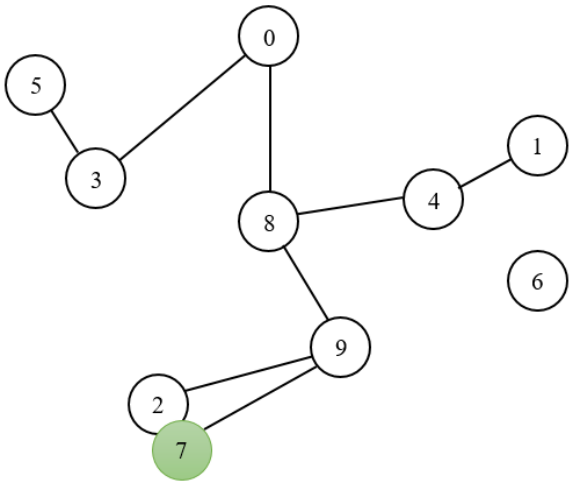

Рисунок 2. Приклад зв'язності у безпроводовій сенсорній мережі після розрахунку довірених вузлів

Вузол, зображений іншим кольором, визначений як довірений на основі їхньої обчислювальної потужності та енергетичних запасів, які перевищують встановлені порогові значення. Цей вузол може бути використаний для маршрутизації даних в мережі, забезпечуючи надійність і безпеку передачі даних[11].

Крок 4. Використання RSSI для визначення довірених вузлів у безпроводових сенсорних мережах

При проведені розрахунків відстаней між вузлами для мереж з різною кількістю вузлів, використовується формула відстані на основі сили сигналу (RSSI).

Для кожної мережі можна зробити припущення, що вихідна потужність сигналу передавача (P_t) і константа зсуву (L) мають певні стандартні значення, і що RSSI вимірюється для кожного вузла.

Після цього, можна відобразити отримані відстані на графіку. Доцільно припустити, що P_t і L мають постійні значення, а значення RSSI випадкові, що відображає різні відстані між вузлами [12]. Для коефіцієнта затухання сигналу n, можна обрати середнє значення, що дорівнює 3.

На рис. 3. відображено розрахункові відстані між вузлами на основі модельних значень RSSI. Кожна точка на графіку відповідає певному вузлу з його значенням RSSI та розрахованою відстанню до інших вузлів.

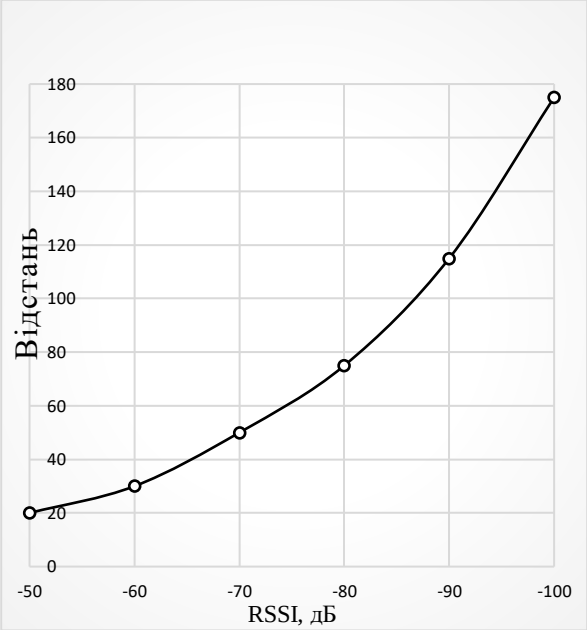

Рисунок 3. Графік відстані між вузлами на основі модельних значень RSSI

З рис. 3 можна зробити висновок, що при вищому значені RSSI (менша відстань до передавача), фіксується менша відстань до вузла, а при нижчому RSSI (більша відстань від передавача) – більшу відстань до вузла.

Точки розподілені вздовж кривої, яка відображає зворотну залежність між RSSI та відстанню. Збільшення кількості вузлів може призводити до збільшення густини точок на графіку, що відображає більшу кількість можливих відстаней між вузлами у мережі з більшою кількістю вузлів.

Значення відстаней виражені у відповідних одиницях, а RSSI – в децибелах (дБ/dBm). З рис. 3. робимо висновок, що відстані збільшуються зі зменшенням значень RSSI, що відповідає очікуваному спаду сигналу зі збільшенням відстані.

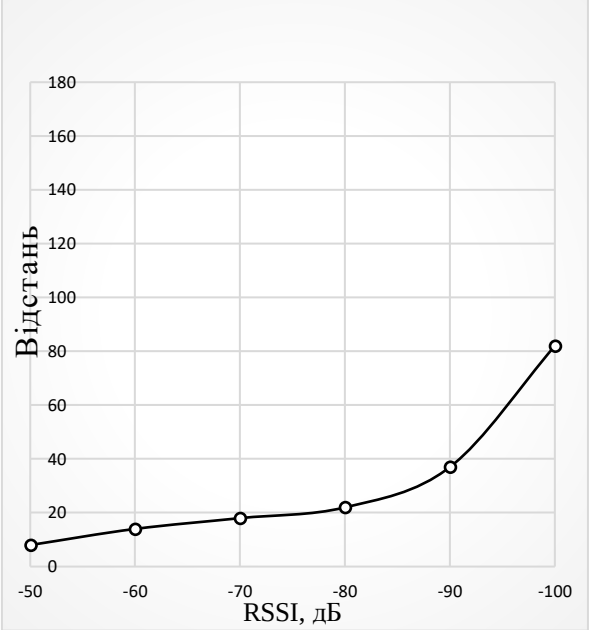

Рисунок 4. Графік відстані між вузлами на основі модельних значень RSSI при створенні списку довірених вузлів

Рис. 4. допомагає візуалізувати, як RSSI може бути використано для визначення відстані в безпроводових сенсорних мережах, що є ключовим для виявлення всіх сусідніх вузлів при створенні списку довірених вузлів.

Обговорення

Порівнюючи рис. 3 та рис. 4., а саме розрахункові відстані між вузлами з двох різних мереж: одна з вузлами, до яких застосовано алгоритм, і "звичайна" мережа без алгоритму. Можна зробити висновок, що для "звичайної" мережі точки мають більші значення RSSI і відповідно менші відстані, що може бути результатом використання вузлів із слабшими сигналами або більшими відстанями.

Це демонструє, як підхід щодо створення списку довірених вузлів може допомогти у відсіванні вузлів із слабкими сигналами, тим самим підвищуючи надійність комунікації в мережі, оскільки вузли з більшими відстанями можуть потребувати більше енергії для передачі даних або можуть мати більшу ймовірність втрати даних.

Висновки

Таким чином, в сучасних умовах постійного збільшення щільності та проникнення безпроводових сенсорних технологій та їх складових елементів у різні сфери життєдіяльності, безперервно зростає й важливість інформаційної безпеки, особливо у військовій сфері. Пов'язано це з підвищенням ризиків неавторизованого доступу та інших варіантів втручання, які можуть підривати приватність та цілісність даних у БСМ.

Своєю чергою, впровадження метрики сили сигналу RSSI для визначення відстаней між вузлами сприяє формуванню списків довірених вузлів, що підвищує ефективність комунікації в мережі. Зазначений процес дозволяє ідентифікувати та відокремлювати вузли з недостатньою сигнальною потужністю, оптимізуючи енергетичне споживання та мінімізуючи ризики втрати даних. Тому адекватне управління довіреними вузлами і ключами, а також ефективне розпорядження ресурсами є вирішальними для забезпечення стабільності та безпеки мережевих операцій у БСМ.

Напрямами подальших досліджень є побудова функціональної моделі підсистеми управління безпекою з урахуванням запропонованого комплексного підходу, реалізація якого дозволить запобігти зростаючим викликам і загрозам.

Список використаних джерел

1. Dovzhenko N., Barabash O., Ausheva A., Ivanichenko Y., Obushnyi S.. Comprehensive Analysis of Efficiency and Security Challenges in Sensor Network Routing. CEUR Workshop Proceedings, Volume 3550, Cybersecurity Providing in Information and Telecommunication Systems, CPITS-II 2023. Pp. 275-280.

2. Машталір В.В., Жук О.В., Міненко Л.М., Артюх С.Г. Концептуальні підходи застосування бездротових сенсорних мереж арміями передових країн світу. Сучасні інформаційні технології у сфері безпеки та оборони. 2023. Т. 47, No2. С. 96–112.

3. Міночкін А.І., Романюк В.А., Жук О.В. Перспективи розвитку тактичних сенсорних мереж. Збірник наукових праць ВІТІ НТУУ "КПІ". 2007. No2. С. 112–119.

4. Міночкін А.І., Романюк В.А. Безпека мобільних радіомереж. Збірник наукових праць ВІТІ НТУУ "КПІ". 2004. No 5. С. 116–26.

5. Міночкін А.І., Романюк В.А., Шаціло П.В. Виявлення атак в мобільних радіомереж. Збірник наукових праць. ВІТІ НТУУ "КПІ". 2005. No 1. С. 102–111.

6. Amine Kardi. Rachi Zagrouba. Attacks classification and security mechanisms in Wireless Sensor Networks. Advances in Science, Technology and Engineering Systems Journal. 2019. Vol. 4. No 6. P. 229–243.

7. Kobzev, V., Vasilyev, V., Doska, O. and Fomenko, D. 2019. Problematic issues and perspective ways for ensuring documentation of battle work on combat means of surface-to-air missile systems (complexes). Journal of Scientific Papers "Social development and Security". 9, 1 (Mar. 2019), 17-25.

8. Бондарчук А.П., Бржевська З.М., Макаренко А.О., Собчук В.В. Дослідження проблематики функціонування алгоритму передачі інформації при наявності прихованих вузлів в безпроводових сенсорних мережах/ А.П. Бондарчук, З.М. Бржевська, Н.М. Довженко, А.О. Макаренко, В.В. Собчук // Кібербезпека: освіта, наука, техніка. – 2019. №4(4). – С. 54-61.

9. Haidur H., Brzhevska Z., Ivanichenko Y., Nesterova O. Method of Sensor Network Functioning under the Redistribution Condition of Requests between Nodes. CEUR Workshop Proceedings. Volume 3421, Cybersecurity Providing in Information and Telecommunication Systems, CPITS 2023. P. 278–283.

10. Hu Z., Mukhin V., Kornaga Y., Barabash O., Herasymenko O. Analytical Assessment of Security Level of Distributed and Scalable Computer Systems. International Journal of Intelligent Systems and Applications, 2016. Vol. 8. No. 12. Hong Kong: MECS Publisher, 2016. P. 57 – 64.

11. Довженко Н. М., Саланда І. П., Барабаш А. О., Коваль М. О. Дослідження методики передачі інформації в безпроводових сенсорних мережах між інтелектуальними сенсорними датчиками. Science and Education a New Dimension. Natural and Technical Sciences, VII(23), Issue: 193, 2019 Feb. Budapest. p.39-42.

12. Barabash O., Ausheva N., Obidin D., Musienko A., Fedchuk T. Development of a hybrid network traffic load management mechanism using smart components. 2023 IEEE 7th International Conference on Methods and Systems of Navigation and Motion Control (MSNMC). October 24 – 27, 2023, Kyiv, National Aviation University, Ukraine. P. 38 – 41.

[1]**Pavlo Openko** **(PhD, Senior Researcher)**
https://orcid.org/0000-0001-7777-5101
[2]**Nadiia Dovzhenko** **(PhD, Associated Professor)**
https://orcid.org/0000-0003-4164-0066
[1]**Pavlo Orikhovskyi**
https://orcid.org/0000-0003-4309-154X
[1]**Dmytro Ikaiev** **(PhD)**
https://orcid.org/0000-0002-3501-0642

[1]***The National Defence University of Ukraine, Kyiv, Ukraine***
[2]***National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine***

ENSURING RELIABILITY AND SECURITY IN MODERN WIRELESS SENSOR NETWORKS BASED ON THE IMPLEMENTATION OF THE RSSI METRIC

In recent decades, wireless sensor networks (WSNs) have undergone significant transformations. In particular, this became possible thanks to the progress in technology, the miniaturization of components and the growth of computing power. Sensor networks usually consist of a large number of low-power multifunctional devices that are deployed in a certain geographical area. Although most of the elements of such a network have limited physical resources, combined together, they are quickly configured to perform a number of functional tasks in the field of science, technology, protection of critical infrastructure, protection and monitoring of the environment, etc.

However, with the development and transformation of BSM, the issue of information security is increasingly being investigated, as the risks of unauthorized access or interference can seriously undermine the effectiveness and reliability of these technologies. It is appropriate to note that precisely because of the open environment of transmission of signals and information, it is necessary to improve, develop and implement updated and advanced methods of encryption and authentication to ensure confidentiality and integrity of data. In addition, the development of mechanisms for detecting and responding to attacks in sensor networks is becoming critical. All this is required to maintain the stability and security of both individual sensor sensors and nodes, as well as the entire network as a whole.

Keywords: *sensor networks, wireless sensor networks, information security, data, unmanned aerial vehicle, reliability, nodes, sensors.*

References

1. Dovzhenko N., Barabash O., Ausheva A., Ivanichenko Y., Obushnyi S.. Comprehensive Analysis of Efficiency and Security Challenges in Sensor Network Routing. CEUR Workshop Proceedings, Volume 3550, Cybersecurity Providing in Information and Telecommunication Systems, CPITS-II 2023. Pp. 275-280.

2. Mashtalir V.V., Zhuk O.V., Minenko L.M., Artjukh S.Gh. Konceptualjni pidkhody zastosuvannja bezdrotovykh sensornykh merezh armijamy peredovykh krajin svitu. Suchasni informacijni tekhnologhiji u sferi bezpeky ta oborony. 2023. T. 47, No2. S. 96–112.

3. Minochkin A.I., Romanjuk V.A., Zhuk O.V. Perspektyvy rozvytku taktychnykh sensornykh merezh. Zbirnyk naukovykh pracj VITI NTUU "KPI". 2007. No2. S. 112–119

4. Minochkin A.I., Romanjuk V.A. Bezpeka mobiljnykh radiomerezh. Zbirnyk naukovykh pracj VITI NTUU "KPI". 2004. No 5. S. 116–26.

5. Minochkin A.I., Romanjuk V.A., Shacilo P.V. Vyjavlennja atak v mobiljnykh radiomerezh. Zbirnyk naukovykh pracj. VITI NTUU "KPI". 2005. No 1. S. 102–111

6. Amine Kardi. Rachi Zagrouba. Attacks classification and security mechanisms in Wireless Sensor Networks. Advances in Science, Technology and Engineering Systems Journal. 2019. Vol. 4. No 6. P. 229–243.

7. Kobzev, V., Vasilyev, V., Doska, O. and Fomenko, D. 2019. Problematic issues and perspective ways for ensuring documentation of battle work on combat means of surface-to-air missile systems (complexes). Journal of Scientific Papers "Social development and Security". 9, 1 (Mar. 2019), 17-25.

8. Bondarchuk A.P., Brzhevsjka Z.M., Makarenko A.O., Sobchuk V.V. Doslidzhennja problematyky funkcionuvannja alghorytmu peredachi informaciji pry najavnosti prykhovanykh vuzliv v bezprovodovykh sensornykh merezhakh/ A.P. Bondarchuk, Z.M. Brzhevsjka, N.M. Dovzhenko, A.O. Makarenko, V.V. Sobchuk // Kiberbezpeka: osvita, nauka, tekhnika. – 2019. - #4(4). – S. 54-61.

9. Haidur H., Brzhevska Z., Ivanichenko Y., Nesterova O. Method of Sensor Network Functioning under the Redistribution Condition of Requests between Nodes. CEUR Workshop Proceedings. Volume 3421, Cybersecurity Providing in Information and Telecommunication Systems, CPITS 2023. P. 278–283.

10. Hu Z., Mukhin V., Kornaga Y., Barabash O., Herasymenko O. Analytical Assessment of Security Level of Distributed and Scalable Computer Systems. International Journal of Intelligent Systems and Applications, 2016. Vol. 8. No. 12. Hong Kong: MECS Publisher, 2016. P. 57 – 64.

11. Dovzhenko N. M., Salanda I. P., Barabash A. O., Kovalj M. O. Doslidzhennja metodyky peredachi informaciji v bezprovodovykh sensornykh merezhakh mizh intelektualjnymy sensornymy datchykamy. Science and Education a New Dimension. Natural and Technical Sciences, VII(23), Issue: 193, 2019 Feb. Budapest. p.39-42.

12. Barabash O., Ausheva N., Obidin D., Musienko A., Fedchuk T. Development of a hybrid network traffic load management mechanism using smart components. 2023 IEEE 7th International Conference on Methods and Systems of Navigation and Motion Control (MSNMC). October 24 – 27, 2023, Kyiv, National Aviation University, Ukraine. P. 38 – 41.