Проблеми безпеки у функціонально стійких бездротових сенсорних мережах

А. В. Собчук[1], А. О. Барабаш[2], Ю. В. Кравченко[1], М. О. Коваль[1]

[1]КНУ ім.Тараса Шевченка
[2]Національний технічний університет України "Київський політехнічний @інститут імені Ігоря Сікорського
Corresponding author. E-mail: anri.sobchuk@gmail.com, andrew.barbsh@gmail.com

Paper received 25.01.19; Accepted for publication 06.01.19.

https://doi.org/10.31174/SEND-NT2019-193VII23-10

Анотація. У роботі досліджено основні вимоги та критерії інформаційної безпеки для функціонально стійких бездротових сенсорних мереж. Розглянуто основні загрози та види атак на бездротові сенсорні мережі відповідно до кожного з рівнів функціонування мережі. Розглянуто підходи, що дозволяють підвищити показники функціональної стійкості нівелюючи основні загрози інформаційної безпеки.

Ключові слова: *бездротова сенсорна мережа, безпека, функціональна стійкість.*

Вступ. За останнє десятиріччя широкого поширення набули бездротові сенсорні мережі (БСМ). Бездротова сенсорна мережа являє собою розподілену систему збору, зберігання і обробки інформації [1]. Для забезпечення безперервного надійного функціонування сенсорної мережі в автономному режимі на тривалих термінах експлуатації пропонується забезпечити в системі властивість функціональної стійкості. В цьому випадку система буде нечутливою до зовнішніх та внутрішніх дестабілізуючих чинників, виконувати основні функції моніторингу зовнішнього середовища та передачі сукупності параметрів до центральної станції обробки і аналізу інформації [2]. На сьогодні особливо актуальним є питання безпеки і конфіденційності даних у БСМ. Головна відмінність бездротових мереж від проводових пов'язана з неконтрольованою областю передачі даних між кінцевими точками мережі. Це дає змогу зловмисникам, що перебувають в безпосередній близькості від бездротових структур, завдавати атаки, які були неможливими у проводових типах мереж[3].

Аналіз публікацій та відомих положень існуючої теорії функціональної стійкості виявив, що було сформульовано та доведено загальну відмінність стійкості функціонування від функціональної стійкості: стійкість функціонування характеризує поведінку координат незбуреного та збуреного руху системи, а функціональна стійкість характеризує відхилення основних функцій систем під час впливу на неї зовнішніх та внутрішніх дестабілізуючих факторів [4].

Питання функціонування існуючих протоколів в бездротових мережах розглядаються багатьма вченими. Проблеми забезпечення енергоефективності вирішувались у [5,6]. Типи атак та вплив кожної з них на сенсорні мережі досліджували в [7]. Аналіз загроз та механізмів забезпечення інформаційної безпеки в бездротових сенсорних мережах досліджувався в роботі [8].

Однак дані роботи не в повній мірі розглядають загрози інформаційної безпеки відповідно до кожного рівня функціонування мережі з точки зору теорії функціональної стійкості.

Матеріали та методи. Матеріальним підґрунтям для аналізу стали фахові збірники наукових праць.

Мета. Метою роботи є аналіз існуючих проблем безпеки БСМ на кожному з рівнів функціонування, огляд існуючих методів протидії для забезпечення надмірності: структурної, часової, інформаційної, функціональної, навантажувальної і т.д.. **Результати та їх обговорення.** Теорія функціональної стійкості (ФС) складних систем дозволяє забезпечити найбільшу ефективність системи в умовах впливу на неї дестабілізуючих чинників.

Виділяється три рівні забезпечення ФС: концептуальний, системно-функціональний, організаційно-технічний.

Концептуальний рівень визначає комплекс завдань, пов'язаних з розробкою структури та визначенням вмісту такої концепції, а саме: 1) визначення комплексу властивостей, складових ФС; 2) формування системи показників і критеріїв ФС; 3) обґрунтування вимог до ФС; 4) визначення видів загроз порушення працездатності системи і можливих сценаріїв впливу загроз різних видів; 5) організація протидії загрозам порушення працездатності систем.

Системно-функціональний рівень. Система забезпечення ФС повинна створюватися на етапі проектування БСМ і враховувати особливості побудови і функціонування останньої в умовах впливу дестабілізуючих факторів. Ця обставина вимагає розробки комплексної моделі функціонування БСМ. Така модель в загальному вигляді може бути представлена як: $G = I, \mu$, де I – модель БСМ; μ – модель впливу дестабілізуючих факторів [4].

Узагальнена функціональна архітектура сенсорної мережі визначає функціональні компоненти мережі та зв'язки між ними, які повинні бути присутні у мережі, розподіл обов'язків між елементами для підтримки функцій мережі – як зовнішніх, так і внутрішніх.

Так як, однією з функцій БСМ є збір та аналіз даних, архітектура БСМ ґрунтується на еталонній моделі OSI. Однак, на практиці мережева взаємодія елементів БСМ реалізується на п'яти рівнях функціонування: прикладному, транспортному, мережевому, рівні передачі даних та фізичному рівні. Також прийнято виділяти три допоміжні рівні функціонування, що виконують суміжні функції, а саме: рівень управління енергоресурсами, рівень управління даними / процесами, рівень управління мобільністю.

Існують певні архітектурні відмінності між найбільш поширеними моделями: OSI, WLAN і WSN(БСМ), що представлені в таблиці 1 [10].

Таблиця 1. Порівняльна таблиця рівнів функціонування моделей OSI, WLAN та WSN (БСМ)

WSN(БСМ)	WLAN	OSI
БСМ прикладний рівень	Прикладні програми	Прикладний рівень
БСМ проміжне програмне забезпечення	Проміжне програмне забезпечення	Рівень представ-влення даних
-	Сокетний API	Сеансовий рівень
БСМ транспортні протоколи	TCP/UDP	Транспортний рівень
БСМ прото-коли маршру-тизації	IP	Мережевий рівень
Контроль помилок передачі, БСМ MAC протоколи	WLAN адаптери та драйвери, WLAN MAC протоколи	Рівень передачі даних
Приймач-передавач	Приймач-передавач	Фізичний рівень

На основі вище наведених даних доцільно дослідити кожен з рівнів функціонування БСМ для забезпечення максимальних показників функціональної стійкості мережі. З точки зору інформаційної безпеки - це досягнення конфіденційності даних, їх цілісності та доступності даних.

Для БСМ це означає, що різні режими функціонування елементів мережі дозволяють використовувати інформаційні ресурси відповідно до правил, встановлених політикою безпеки. Однак, на сьогодні існує багато видів загроз, кожну з яких потрібно розглядати на окремому рівні функціонування мережі.

Таблиця 2. Види атак на кожен з рівнів БСМ та способи протидії ним

Рівні	Види атак	Способи захисту
Фізичний	Створення перешкод	Розподіл спектру, пріоритетність повідомлень, топографічна розмітка, зміни режиму
Передачі даних	Колізії, виснаже-ння ресурсів ме-режі, фальсифі-кація даних	Вдосконалення ПЗ, зменшення розміру кадрів, обмеження вхідного/вихі-дного трафіку
Мереже-вий	HelloFlood Attack; Атака «бездонна воронка» (Sink Hole Attack); Атака «Червото-чина» (WormHole Attack); вибіркова розсилка (Selec-tive Forwarding / GreyHole); «Зача-роване» атака (Sybil Attack); Атака «Чорна діра »(Black Hole Attack), сфальси-фіковані (Spoo-fed),змінена (Altered) або пов-торена (Replayed) інформація про маршрутизації.	Фільтрація трафіку,налаш-тування базової антен-тифікація та моніторинг, виявлення надмірностей в передачі даних, резер-вування каналу передачі,навігація передачі пакетів за допомогою географічного розташування, перевірка дво-направлених посилань
Транс-портний	Десинхронізація, Dos, DDoS, Flooding	Автенти-фікація (в т.ч. двофакторна)

Слід зазначити, що прикладний рівень та типи атак на нього охоплює широкий спектр задач інформаційної безпеки, що слід розглядати окремо, в залежності від ПЗ, ОС та багатьох інших компонентів мережі.

Забезпечення функціональної стійкості відбувається в три етапи [2]:

- виявлення позаштатної ситуації
- локалізація позаштатної ситуації
- відновлення функціонування систем з обмеженими можливостями

Реалізація функціональної стійкості досягається застосуванням у складній технічній системі різних уже існуючих видів надмірності (структурної, часової, інформаційної, функціональної, навантажувальної та ін.) шляхом перерозподілу ресурсів з метою парирування наслідків позаштатних ситуацій [9].

Найбільш поширеними типами атак на сьогодні є атаки на мережевий та транспортний рівні функціонування БСМ. Розглянемо більш детально дестабілізуючі фактори впливу на кожен з них.

Транспортний рівень. В залежності від розміру мережі варіюється її здатність до захисту від таких дестабілізуючих факторів, як DOS-атаки. Багатоканальні алгоритми, в таких ситуаціях, забезпечують кращий захист, у випадку великого розміру мережі, *створюючи необхідну надмірність* (надлишкові шляхи передачі сигналу). Багатоканальний (багатопотоковий) підхід виявляється найменш ефективним для малих мереж, в яких кожен вузол має малу кількість сусідів та альтернативних шляхів до базової станції [11].

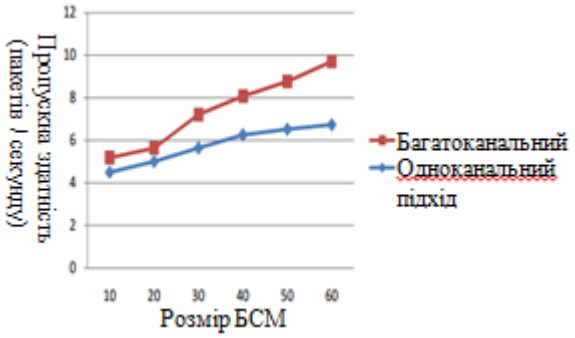

Рис. 1. Значення пропускної здатності БСМ за використання багато- та одноканального підходу передачі даних

Мережевий рівень. Загалом, методи виявлення атак можна розділити на дві основні категорії, а саме: централізовані та розподілені. Кожен з них є більш пріоритетним в залежності від типу розташування вузлів БСМ: локального чи мобільного. Локальне

розташування вузлів не передбачає зміни їх місця розташування, що дозволяє відслідковувати їхній стан та заздалегідь прогнозувати можливі дестабілізуючі фактори. В той же час мобільна БСМ дозволяє скоригувати необхідні обчислювальні ресурси та покривати значно більшу площу поширення. Саме останній тип БСМ є більш вразливим з точки зору інформаційної безпеки та стабільного функціонування в цілому.

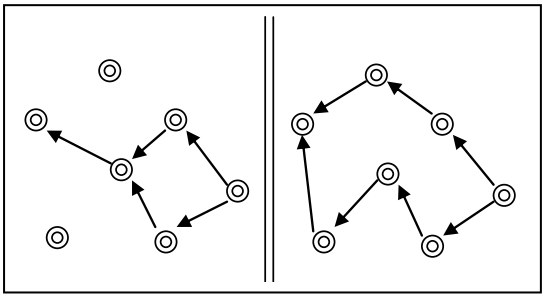

Рис. 2. Візуальна схема багато- та одноканального підходу передачі даних

Мережевий рівень. Загалом, методи виявлення атак можна розділити на дві основні категорії, а саме: централізовані та розподілені. Кожен з них є більш пріоритетним в залежності від типу розташування вузлів БСМ: локального чи мобільного. Локальне розташування вузлів не передбачає зміни їх місця розташування, що дозволяє відслідковувати їхній стан та заздалегідь прогнозувати можливі дестабілізуючі фактори. В той же час мобільна БСМ дозволяє скоригувати необхідні обчислювальні ресурси та покривати значно більшу площу поширення. Саме останній тип БСМ є більш вразливим з точки зору інформаційної безпеки та стабільного функціонування в цілому.

Однією з найпоширеніших атак на БСМ є атака реплікації (підробки) вузла. Особливо уразливими до даного виду загроз є мережі з мобільними вузлами. Після захоплення вузла зловмисник збирає всі облікові дані, такі як: ключі та ідентифікаційна інформація, тощо. Нападник може перепрограмувати його і реплікувати вузол, щоб прослухати передані повідомлення або поставити під загрозу функціональність мережі.

Метод визначення	Техноло-гія	Алгорит-мічна склад-ність методу	Алгоритмічна складність затрат обчис-лювальних ресурсів
SRPT	Speed based	O(n√n)	O(n)
A new protocol	Key based	O(n log n)	-
XED	Random number based	O(1)	O(4 • d • E|X|)
EDD	Node meeting based	O(1)	O(n)
SEDD	Node meeting based	O(n)	O(ζ)
UTLSE	Time location based	O(n)	O(√n)
MTLSD	Time location based	O(n)	O(√n)
Patrol Detection	Distanse based	O(n)	-
Theory and Approaches	Token based	O(n) & O(n • √k)	-
SHD	fingerprint	-	-
XED	Localized based	O(1)	O(n)
EDD	Localized based	O(1)	O(1)

Таблиця 3. Методи та необхідні ресурси для визначення атак реплікації на БСМ з мобільними вузлами [9].

Таким чином застосування методів визначення атак спрямованих на мережевий рівень, що мають найменшу асимптотичну складність забезпечує функціональну стійкість у три етапи: виявлення позаштатної ситуації, локалізація позаштатної ситуації, відновлення функціонування систем з обмеженими можливостями.

Висновки. У статті розглянуто головні загрози безпеки БСМ відповідно до кожного з рівнів функціонування, можливі методи протидії ним, що відповідають усім етапам забезпечення функціональної стійкості та необхідного рівня надмірності: структурної, часової, інформаційної, функціональної, навантажувальної.

ЛІТЕРАТУРА

1. Галкін П. В. Аналіз моделей та оптимізації збору інформації в бездротових сенсорних мережах [Електронний ресурс] / П. В. Галкін // Восточно-Европейский журнал передовых технологий. – 2014. – Режим доступу до ресурсу:http://journals.uran.ua/eejet/article/viewFile/28008/25490.
2. Собчук А.В. Математична модель функціонально стійкої безпровідної сенсорної мережі / А.В. Собчук, М.О. Коваль, Ю.В. Кравченко, О.В. Барабаш // Наукове періодичне видання «Системи управління, навігації та зв'язку». – Полтава: ПНТУ, 2017. – Вип. 6 (46). – С. 122 – 126
3. Щелконогов О. О. Забезпечення захисту бездротової системи контролю розкриття апаратури [Електронний ресурс] / О. О. Щелконогов // Автоматика, вимірювання та керування. – 2012. – Режим доступу до ресурсу:http://ena.lp.edu.ua/bitstream/ntb/21459/1/36-192-197.pdf.
4. Кравченко Ю. В. Визначення проблематики теорії функціональної стійкості щодо застосування в комп'ютерних системах / Ю. В. Кравченко, С. В. Нікіфоров. // Телекомунікаційні та інформаційні технології. – 2014. – №1. – С. 12–18.
5. Heinzelman, W.R. Energy-Efficient Communication Protocol for Wireless Microsensor Networks / W.R. Heinzelman,

A.Chandrakasan , and H.Balakrishnan // IEEE Proceedings of the 33rd Hawaii International Conference on System Sciences. - 2000. - 1–10 pp.
6. Sohrabi, K. Protocols for Self-Organization of a Wireless Sensor Network / K. Sohrabi, J.Gao , V.Ailawadhi and G.J. Pottie // Personal Communications, IEEE. - October 2000. - Vol. 7. - N5. - 16–27 pp.
7. Баскаков С. С. Исследование способов повыше- ния эффективности маршрутизации по виртуаль- ным координатам в беспроводных сенсорных се- тях // Вестник МГТУ им. Баумана. Сер. Приборо- строение. 2009. № 2. С. 112–124
8. Аналіз загроз та механізмів забезпечення інформаційної безпеки в сенсорних мережах / [О. Г. Корченко, М. Б. Алєксандр, Р. С. Одарченко та ін.]. // Науково-практичний журнал "Захист інформації". – 2016. – С. 48–56.
9. Неділько С.М. Технологічні основи забезпечення функціональної стійкості автоматизованої системи управління повітряним рухом / С.М.Неділько, Г.Л.Бара-нов // Авиационно-космическая техника и технология. –Х.: "ХАІ", 2011. – No.9 (86). – С. 202 – 206.
10. Alkhatib A. Wireless Sensor Network Architecture / A. Alkhatib, G. Baicher. // International Conference on Computer Networks and Communication Systems. – 2012. – №12
11. Hubboub H. Denial of Service Attack in Wireless Sensor Networks [Електронний ресурс] / Huda Bader Hubboub. – 2010. – Режим доступу до ресурсу: http://library.iugaza.edu.ps/thesis/92125.pdf.

REFERENCES

1. Halkin P. V. Analiz modeley ta optymizatsiyi zboru informatsiyi v bezdrotovykh sensornykh merezhakh [Elektronnyy resurs] / P. V. Halkin // Vostochno-Evropeyskyy zhurnal peredovykh tekhnolohyy. – 2014. – Rezhym dostupu do resursu:http://journals.uran.ua/eejet/article/viewFile/28008/25490.
2. Sobchuk A.V. Matematychna model′ funktsional′no stiykoyi bezprovidnoyi sensornoyi merezhi / A.V. Sobchuk, M.O. Koval′, YU.V. Kravchenko, O.V. Barabash // Naukove periodychne vydannya «Systemy upravlinnya, navihatsiyi ta zv'yazku». – Poltava: PNTU, 2017. – Vyp. 6 (46). – S. 122 – 126
3. Shchelkonohov O. O. Zabezpechennya zakhystu bezdrotovoyi systemy kontrolyu rozkryttya aparatury [Elektronnyy resurs] / O. O. Shchelkonohov // Avtomatyka, vymiryuvannya ta keruvannya. – 2012. – Rezhym dostupu do resursu:http://ena.lp.edu.ua/bitstream/ntb/21459/1/36-192-197.pdf.
4. Kravchenko YU. V. Vyznachennya problematyky teoriyi funktsional′noyi stiykosti shchodo zastosuvannya v komp″yuternykh systemakh / YU. V. Kravchenko, S. V. Nikiforov. // Telekomunikatsiyni ta informatsiyni tekhnolohiyi. – 2014. – №1. – S. 12–18.
7. Baskakov S. S. Yssledovanye sposobov povyshe- nyya éffektyvnosty marshrutyzatsyy po vyrtual′- nym koordynatam v besprovodnykh sensornykh se- tyakh // Vestnyk MHTU ym. Baumana. Ser. Pryboro- stroenye. 2009. № 2. S. 112–124
8. Analiz zahroz ta mekhanizmiv zabezpechennya informatsiynoyi bezpeky v sensornykh merezhakh / [O. H. Korchenko, M. B. Alyeksandr, R. S. Odarchenko ta in.]. // Naukovo-praktychnyy zhurnal "Zakhyst informatsiyi". – 2016. – S. 48–56.
9. Nedil′ko S.M. Tekhnolohichni osnovy zabezpechennya funktsional′noyi stiykosti avtomatyzovanoyi systemy upravlinnya povitryanym rukhom / S.M.Nedil′ko, H.L.Bara-nov // Avyatsyonno-kosmycheskaya tekhnyka y tekhnolohyya. – KH.: "KHAI", 2011. – No.9 (86). – S. 202 – 206.

Security problems in functional sustainable wireless sensor networks

A. V. Sobchuk

Abstract. The paper deals with main requirements and criteria for information security of functionally stable wireless sensor networks. It gives a detailed review of main threats and types of attacks on wireless sensor networks according to each of the levels of network operation. Approaches are considered that allow to increase indicators of functional stability, leveling out the main threats of information security.

Keywords: *wireless sensor network, security, functional stability.*