DOI:**10.33099/2311-7249/2023-48-3-11-19**

УДК: 004.056:076

Артюх Сергій Григорович [1]
Жук Олександр Володимирович *(доктор технічних наук, доцент)* [2]
Чернега Володимир Миколайович *(кандидат технічних наук, доцент)* [2]

[1] ***Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна***
[2] ***Національний університет оборони України, Київ, Україна***

КЛАСИФІКАЦІЯ АТАК У БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖАХ ТАКТИЧНОЇ ЛАНКИ УПРАВЛІННЯ ВІЙСЬКАМИ

Сьогодні активно застосовуються безпроводові сенсорні мережі для розвідки і спостереження, оперативного збору інформації про обстановку, що передається до пунктів управління для аналізу та прийняття рішень у реальному часі. Вирішення питань захисту інформації під час використання сенсорів постають на перший план у процесі ведення бойових дій. Метою статті є удосконалення класифікації атак у безпроводових сенсорних мережах тактичної ланки управління військами на основі проведеного аналізу існуючих вразливостей для забезпечення безпеки таких мереж. Під час написання статті застосовано теоретичні методи, а саме аналіз досліджень і публікацій за тематикою розвитку та впровадження безпроводових сенсорних мереж у воєнній сфері, аналіз існуючих атак на такі мережі та синтез класифікації атак на безпроводові сенсорні мережі тактичної ланки управління військами. Зазначений методологічний підхід дає змогу розробити методи протидії атакам та удосконалити механізми захисту безпроводових сенсорних мереж тактичної ланки управління. У роботі проведено аналіз вразливостей, що визначаються особливостями архітектури безпроводових сенсорних мереж і протоколами їх функціонування. Описано основні та додаткові вимоги з безпеки таких мереж. Наведено удосконалену класифікацію атак у безпроводових сенсорних мережах за такими ознаками як характер дій, рівень моделі відкритих систем, мета впливу, об'єкт управління, позиціонування відносно мережі, тип атакуючого пристрою. На основі запропонованої класифікації проведено аналіз існуючих атак у безпроводових сенсорних мережах тактичної ланки управління військами. Новизною роботи є те, що проведено удосконалення класифікації атак на мобільні радіомережі за порушенням конфіденційності, цілісності, доступності, автентифікації та виснаження ресурсів. Вперше запропоновано класифікацію атак за впливом на різні об'єкти системи управління (підсистемами управління моніторингом, топологією, маршрутизацією, енергоресурсами вузлів, радіоресурсами, якістю обслуговування). Відповідно до запропонованої класифікації розкрито сутність атак на безпроводові сенсорні мережі тактичної ланки управління військами та запропоновано механізми захисту від них. Проаналізовані вразливості та наведена класифікація сприяють поглибленню наукових знань стосовно безпеки систем управління безпроводових сенсорних мереж тактичної ланки управління військами. Прикладне використання ознак класифікації атак сприятиме розробленню архітектури побудови (функціональної моделі) підсистеми управління безпекою з урахуванням особливостей характеристик, методів побудови та організації безпроводових сенсорних мереж.

Ключові слова: *тактична ланка управління, автоматизована інформаційна система, безпроводові сенсорні мережі, різнорідні джерела інформації, сенсорні вузли, безпілотні літальні апарати, вразливість, класифікація атак, об'єкти системи управління, механізм захисту.*

Вступ

Постановка проблеми. Безпроводові сенсорні мережі (далі – БСМ) – розподілені мережі (наземні, повітряні, підземні та ін.), що складаються з різнорідних джерел інформації на основі сенсорних вузлів (стаціонарні малогабаритні сенсори, мобільні роботи-сенсори, сенсорні платформи на основі груп (роїв) безпілотних літальних апаратів), з інтегрованими функціями моніторингу навколишнього середовища, обробки і передачі даних. У загальному випадку БСМ є автоматизованою інформаційною системою, що функціонує за рахунок використання великої кількості взаємопов'язаних безпроводових сенсорних вузлів, до складу яких можуть входити один або декілька датчиків (акустичні, сейсмічні, магнітні, інфрачервоні тощо). Ці вузли можуть розташовуватися на значних географічних територіях та здійснюють моніторинг за об'єктами шляхом визначення різних параметрів навколишнього середовища. Інформаційний обмін здійснюється безпосередньо між сенсорними

вузлами та передається на спеціальні базові станції (шлюзи), або ретранслюватися через проміжні сенсорні вузли [1].

Провідними країнами світу активно використовуються БСМ у воєнній сфері для розвідки і спостереження, оперативного збору інформації про обстановку. Сенсори (датчики) дають змогу отримувати різноманітну інформацію з поля бою про наявність, кількість, розміщення і рух особового складу та техніки противника, а також для збору й аналізу інформації про стан навколишнього середовища, (погода, температура повітря, тиск), інші фактори, що впливають на військові дії. Отримана інформація передається до пунктів управління для аналізу та прийняття рішень у реальному часі, що дає змогу оперативно реагувати на зміни обстановки.

Розташування елементів БСМ на місцевості, захист інформації під час передачі даних, а також стійкість до спроб компрометації даних і фізичного знищення мережі, мають важливе значення під час застосування БСМ в зоні проведення бойових дій. Саме тому завдання забезпечення безпеки БСМ та інформації, що циркулює в таких мережах є важливим науковим завданням.

Аналіз останніх досліджень і публікацій. У статті [1] наведено тактико-технічні характеристики сенсорних систем спеціального (військового) призначення, особливості їх функціонування, узагальнено призначення мобільних бездротових сенсорних мереж оперативного рівня, а також розроблено рекомендації щодо впровадження таких систем у вітчизняній військовій сфері та їхнього подальшого інноваційного розвитку.

Функціональна модель системи управління сенсорною мережею запропонована у статті [2], а також обґрунтовано принципи побудови таких систем, їх структура та функції. Авторами розглядаються перспективи розвитку тактичних сенсорних мереж, наведена їх класифікація і вимоги, які висуваються до них.

У роботах [3; 4] 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. Однак у зазначеній роботі не в повному обсязі розглядаються вразливості та атаки стосовно БСМ, а також не враховується їх особливості функціонування та питання безпеки.

У роботі [5] запропоновано класифікацію атак у БСМ за чотирма ознаками, проте авторами не враховуються специфіка застосування БСМ у тактичній ланці управління військами.

Метою статті є удосконалення класифікації атак у безпроводових сенсорних мережах тактичної ланки управління військами на основі проведеного аналізу існуючих вразливостей для забезпечення безпеки таких мереж.

Виклад основного матеріалу дослідження

У контексті інформаційних технологій та захисту інформації вразливість безпеки – це поведінка або набір умов, присутніх у системі, продукті, компоненті або службі, що порушує політику безпеки. Вразливість можна розглядати як слабкість, що може мати наявний або потенційний вплив на безпеку БСМ або певні наслідки від таких впливів. Використовуючи спеціальні механізми і техніки, зловмисники можуть отримати несанкціонований доступ до інформації, що передається в БСМ з метою її добування, знищення, перекручення або блокування.

Вразливості мереж MANET порівняно з проводовими мережами визначається особливостями її архітектури та протоколами функціонування [3]. Крім вразливостей мобільних радіомереж, в БСМ існують специфічні вразливості, що виникають з обмежень ресурсів мереж і особливостей безпроводового зв'язку між вузлами (сенсорами), що робить використання традиційних методів забезпечення безпеки БСМ недостатньо ефективним, а саме:

потреба використання бездротових каналів зв'язку. Використання широкомовного радіоканалу дає змогу зловмиснику створювати активні й пасивні завади, здійснювати перехоплення та аналіз мережевого трафіку, пошкодження пакетів з даними або втрати пакетів навантаженими вузлами;

відсутність фізичного контроля сенсорів. Розгортання мережі на контрольованій ворогом території дає змогу зловмиснику отримати фізичний доступ до компонентів БСМ. За таких умов з'являється можливість підміни, захоплення або знищення вузлів (сенсорів). Водночас перепрограмуванням одного або кількох вузлів реалізуються різні внутрішні атаки спрямовані на перехоплення, відтворення, зміни або прослуховування даних у всій мережі;

децентралізоване управління та масштабованість мереж. Вузли виконують функції кінцевих пристроїв, датчиків, ретрансляторів та маршрутизаторів. Розміри мережі, велика кількість сенсорів та відсутність централізованого управління ускладнюють реалізацію центрів сертифікації, систем виявлення вторгнень, тощо;

динамічна топологія. Використання складних алгоритмів маршрутизації та механізмів самоорганізації вимагає застосування різних протоколів (канального, мережевого та інших рівнів), що мають свої вразливості. Поєднання різних протоколів може привести до реалізації зловмисником більш складних атак;

обмеженість ресурсів вузлів (сенсорів) (ємність батареї, об'єм пам'яті, продуктивність процесора, пропускна здатність радіоканалу тощо). Енергетичні та обчислювальні можливості вузла

ускладнюють реалізацію надійних механізмів безпеки та впровадження стійких криптографічних алгоритмів, оскільки вони є енергозатратними.

Сенсорна мережа має забезпечувати виконання таких основних вимог з безпеки сучасних інформаційних систем [6]:

конфіденційність (confidentiality) – забезпечує обмін інформації тільки між авторизованими вузлами та не дає змогу ознайомлюватись зловмиснику із будь-якими даними в мережі;

цілісність (integrity) – гарантує, що дані не були модифіковані зловмисником на шляху від відправника до одержувача;

доступність (availability) дає змогу використовувати інформацію на вимогу авторизованих користувачів під час деструктивних дії зловмисника на мережу;

автентифікація (authentication) – визначає ідентичність і підтверджує легітимність відправника/одержувача при обміні інформацією між ними.

Враховуючи особливості роботи БСМ та з метою протидії специфічним атакам визначено перелік додаткових вимог [7], а саме:

авторизація (authorization) – запобігає доступу користувача без відповідних повноважень до ресурсів мережі;

неспростовність (non-repudation) – гарантує неможливість відмови вузлів від факту отримання або відправлення повідомлення;

таємність (privacy) – перешкоджає зловмисникам отримати зміст інформації з обмеженим доступом;

актуальність даних (data freshness) – перевіряє новизну та унікальність отриманих даних і забороняє їх повторне надсилання від будь-якого користувача;

пряма секретність (forward secrecy) – забороняє сенсорному вузлу отримувати доступ (читати) нові повідомлення, після його виходу мережі (втрати прав користувача);

зворотна секретність (backward secrecy) – забороняє сенсорному вузлу у процесі нового підключення до мережі, отримувати доступ (читати) раніше передані повідомлення;

стійкість (resilience) – підтримує функціональні можливості мережі, коли частина вузлів скомпрометована;

анонімність (anonymity) – приховує від зловмисника сенсорні вузли, що обмінюються даними;

самоорганізація (self organization) – дає змогу адаптуватись до різних ситуацій кожному окремому вузлу з метою самовідновлення свого місця в топології мережі;

захищена локалізація (secure localization) – перешкоджає зловмиснику визначити точне місцезнаходження сенсорних вузлів;

синхронізація часу (time synchronization) – запобігає втручанню зловмисника в роботу системи часової синхронізації мережі.

Вимоги до безпеки та вразливості, що притаманні БСМ дають змогу зловмисникам реалізувати атаки різних типів, спрямованих на порушення функціонування мережі, окремих сенсорних вузлів, протоколів маршрутизації, радіоканалів тощо.

Атакою на інформаційну систему називається дія або послідовність зв'язаних між собою дій порушника, які призводять до реалізації загрози шляхом використання вразливостей цієї інформаційної системи.

На основі аналізу існуючих вразливостей та вимог з безпеки авторами запропоновано удосконалену класифікацію атак на БСМ за такими ознаками за: характером дій; рівнем OSI; метою впливу; об'єктом управління; позиціонуванням; атакуючим пристроєм (рис. 1)

Наведена на рис. 1 класифікація атак на БСМ дає змогу розробляти більш ефективні методи захисту, що спрямовані на запобігання визначеним видам атак і механізмам протидії загрозам під час проєктування та експлуатації БСМ.

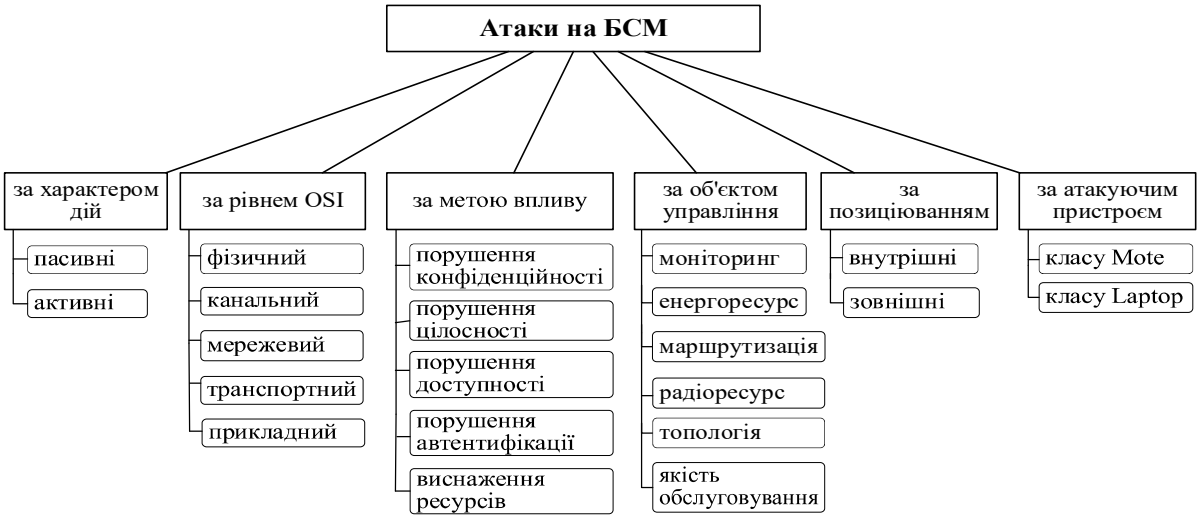

Рисунок 1 – Класифікація атак у безпроводових сенсорних мережах

Відповідно до наведених ознак запропонованої класифікації (рис. 1) розглянемо атаки на БСМ:

За характером дій зловмисника [8].

Пасивні атаки здійснюються шляхом несанкціонованого прослуховування радіоефіру та аналізу мережного трафіка. Пасивні атаки досить складно виявити, оскільки зловмисник не змінює дані, що передаються мережею та не втручається в процес їх передачі. Тому зловмисник має достатньо часу для аналізу інформації та підготовки більш точної та спрямованої атаки.

Активні атаки передбачають втручання зловмисника в процес передачі даних з метою їх зміни, перехоплення або виведення мережі з ладу. Такі атаки можуть призвести до різних наслідків, включно з викраденням чутливих даних, порушення конфіденційності користувачів, зниження ефективності мережі та виведення з ладу її компонентів або мережі в цілому.

За рівнями моделі взаємозв'язку відкритої системи OSI (Open System Interconnection) атаки поділяються відповідно до їх реалізації на кожному з п'яти рівнів еталонної моделі взаємодії відкритих систем характерної для БСМ [9].

Фізичний рівень забезпечує послуги передачі даних радіоканалом та описує його параметри (потужність сигналу, вид модуляції, частоту, тип корегуючого коду, параметри технології множинний вхід – множинний вихід MIMO (Multiple Input – Multiple Output) тощо). Зловмисник реалізовує різні атаки, що спрямовані на порушення конфіденційності даних, виснаження ресурсів, створенню завад для сигналів.

Канальний рівень відповідає за адресацію, доступ до середовища, виявлення та виправлення помилок, надійність з'єднань, мультиплексування та управління потоків даних. Атаки спрямовані на зниження продуктивності мережі та порушення роботи енергозберігаючих протоколів.

Мережевий рівень відповідає за маршрутизацію (призначення адрес, доставку пакетів), топологію та управління навантаженням. Результатами атак можуть бути підміна, переспрямування та зациклення маршрутів, створення перевантаження у вузлах мережі, переповнення маршрутних таблиць, імітація поділу мережі на окремі підмережі, збільшення часу доставки повідомлень.

Транспортний рівень забезпечує управління навантаженням, контроль з'єднання та надійну доставку пакетів у середині БСМ, а також із вузлами зовнішніх мереж. Атаки спрямовані на зменшення пропускної спроможності, повторну передачу пакетів і збільшення кількості помилок у каналі.

Прикладний рівень здійснює контроль функціонування вузлів та обробляє отримані дані за допомогою програмного забезпечення. На цьому рівні використовуються багато протоколів, таких як протокол передачі гіпертекстових документів (HyperText Transfer Protocol (HTTP)) для веб-сервісів, протокол Telnet або Secure Shell (SSH) для віддаленого управління, протокол File Transfer Protocol (FTP) для передачі файлів, Extensible Messaging and Presence Protocol (XMPP) для обміну інформацією між вузлами, простий протокол керування мережею (Simple Network Management Protocol (SNMP)) для моніторингу та відстеження роботи вузлів тощо. Дії зловмисників спрямовуються на порушення синхронізації зв'язку та конфіденційність даних, а також на виявлення вразливостей програмного забезпечення.

За метою впливу атаки в БСМ доцільно розділити на такі класи:

порушення конфіденційності. Зловмисник отримує несанкціонований доступ до мережі та її вузлів разом з переданою інформацією, шляхом прослуховування або захоплення мережевого трафіку або сенсора;

порушення цілісності. Атаки спрямовані на зміну або знищення переданої інформації за допомогою модифікації заголовків пакетів, застосування SQL-ін'єкцій для програмного забезпечення, тощо;

порушення доступності. Атаки спрямовані на перешкоджання нормальному функціонуванню мережі, зниження її продуктивності, часткову або повну втрату доступу до послуг і сервісів; Прикладом таких атаки є DoS атаки;

порушення автентифікації. Атаки спрямовані на отримання доступу до паролів або криптографічних ключів шляхом підробки ідентифікаційних даних користувача, модифікацією ідентифікаторів, фальсифікацією маршрутних даних, тощо;

виснаження ресурсів. Атаки спрямовані на пришвидшення витрат обмежених енергетичних та обчислювальних ресурсів вузлів, що може привести до повного відключення мережі.

За об'єктом управління атаки можуть бути спрямовані на різні підсистеми системи управління мережею.

Атаки спрямовані на підсистему *управління моніторингом* впливають на розгортання, покриття, виявлення та ідентифікацію об'єктів та якість моніторингу.

Атаки на підсистему *управління топологією* перешкоджають побудові та підтримці топології БСМ відповідно до потенційних можливостей та наявних ресурсів мережі.

Атаки спрямовані на підсистему *управління маршрутизацією* впливають на побудову та підтримку маршрутів передачі заданої якості при під час виконання вимог до їх функціонування, типу трафіка, цільових функцій управління.

Результатом атак на підсистему *управління радіоресурсом* може бути порушення розподілу часового, просторового, частотного, кодового ресурсів для забезпечення інформаційного обміну між сусідніми вузлами.

Проведення атак на підсистему *управління якістю обслуговування* перешкоджає передачі

певних класів трафіка із заданою якістю обслуговування (Quality of Service, QoS).

Метою атак на підсистему *управління енергоресурсу* вузлів є збільшення споживаної енергії вузлами мережі на будь-якому рівні еталонної моделі взаємодії відкритих систем.

За позиціюванням зловмисника відносно розгорнутої БСМ атаки розрізняють[10]:

зовнішні атаки, що проводяться неавторизованими пристроями. Вони не входять до складу мереж і намагаються відправити шкідливий трафік або отримати незаконний доступ до мережі.

внутрішні атаки, що здійснюються скомпрометованими вузлами. Вони належать до мережі, та спрямовані на підробку даних, впровадження фальшивих даних у мережу, розповсюдження вірусів та інших шкідливих програм, які можуть пошкодити мережу.

За атакуючим пристроєм виділяють атаки класу вузла (Mote) та класу базової станції (Laptop) [11].

Під час *атак класу Mote* зловмисники використовують пристрої з подібними технічними характеристиками та можливостями апаратного забезпечення до вузлів мережі, щоб виконати шкідливі дії, спрямовані на вплив на функціональні можливості мережі (дані, маршрутизація, шляхи, керування енергією та ін).

Під час *атак класу Laptop* зловмисники використовують спеціальні пристрої з великою дальністю передачі та обчислювальною потужністю, ніж сенсорні вузли мережі. Такі атаки характеризуються складністю, багаторівневістю та загальною небезпечністю для функціонування мережі.

Відповідно до наведеної на рис. 1 класифікації атак в БСМ проведемо групування існуючих атак (табл.1).

Таблиця 1

Відповідність атак в безпроводовій сенсорній мережі до класифікації

Атаки	за характером дій		за рівнями моделі OSI					за метою впливу					за об'єктом управління						за позиціюванням		за атакуючим пристроєм	
	Пасивні	Активні	Фізичний	Канальний	Мережевий	Транспортний	Прикладний	Конфіденційність	Цілісність	Доступність	Автентифікація	Виснаження	Моніторинг	Топологія	Маршрутизація	Радіоресурс	Якість обслуговування	Енергоресурс вузлів	Зовнішні	Внутрішні	Mote	Laptop
Jamming		+	+	+	+				+	+		+		+		+	+	+	+	+	+	+
Physical		+	+					+	+	+			+	+		+			+		+	
Exhaustion		+		+						+		+		+		+	+	+	+	+	+	+
Collision		+		+						+		+	+				+	+	+	+	+	+
Unfairness		+		+						+		+	+	+			+	+	+	+	+	+
Sybil Attack		+		+	+				+	+	+	+		+	+			+		+	+	
Sinkhole		+			+			+	+	+		+	+		+		+	+	+	+	+	+
Hello Flood		+			+					+	+	+		+	+			+	+			+
Selective		+	+		+			+		+		+			+		+	+		+	+	
Black Hole		+			+			+		+	+	+	+		+			+		+	+	+
Wormhole		+			+			+		+		+		+	+			+		+		+
Spoofed Routing Information		+			+			+	+	+		+	+	+	+		+	+		+	+	+
Homing	+	+			+			+			+		+	+					+		+	+
Flooding		+				+				+		+					+	+		+	+	+
Desynchronization attack		+				+				+	+	+	+			+		+		+	+	+
Overwhelm attack		+					+			+		+	+				+	+	+		+	
Path-based DoS		+					+			+		+					+	+		+	+	+
Malware attack		+					+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Monitoring and Eavesdropping	+		+	+	+	+		+											+	+	+	+
Traffic Analysis	+		+	+	+	+		+											+	+	+	+

Створення завад (Jamming). Випромінювання сигналів високої потужності зловмисним вузлом на визначених частотах (діапазоні частот) з метою порушення/блокування радіозв'язку між вузлами. Також створення завад зловмисником можливе надсиланням надлишкових/шкідливих пакетів для порушення обміну повідомлень [12].

Механізми захисту: псевдовипадкове переналаштування робочої частоти (FHSS), захист від повторної передачі, автентифікація, система виявлення вторгнень.

Фізичні атаки (Physical attack). Захоплення зловмисником сенсорного вузла дає змогу отримати доступ до конфіденційних даних (ключів шифрування, методів аутентифікації та програмного коду) і скомпрометувати його для реалізації інших типів атак [13].

Копіювання зловмисником сенсорного вузла передбачає впровадження в мережу скомпрометованого вузла з метою нав'язування фальшивої інформації або розповсюдження шкідливого програмного коду.

Знищення сенсорного вузла порушує організацію і топологію мережі.

Механізми захисту: захист від несанкціонованого доступу до апаратної частини сенсора, використання фізично неклонованих функцій (Physical Unclonable. Function (PUF)).

Виснаження (Exhaustion). Порушення зловмисником функціонування енергозберігаючих протоколів, генерування та безперервне надсилання помилкового інформаційного або службового трафіку сенсорним вузлам для передчасного виснаження енергоресурсів вузлів [14].

Механізми захисту: захист від повторної передачі, аутентифікація на канальному рівні.

Колізії (Collision). Навмисне створення зловмисним вузлом колізій призводить до зменшення пропускної спроможності мережі та блокування зв'язку між вузлами.

Механізми захисту: часове рознесення, алгоритм обчислення контрольної суми.

Нерівномірність доступу (Unfairness). Постійне надсилання зловмисним вузлом великої кількісті пакетів з коротким часом очікування знижує пропускну здатність та погіршує доступність каналу для інших вузлів [15].

Механізми захисту: мультиплексування з часовим поділом, що дозволяє кожному вузлу передавати лише в певному часовому інтервалі.

Атака Сивілли (Sybil attack). Зловмисний вузол використовує фальшиві ідентифікатори та визначається в мережі як декілька окремих вузлів. Можливість збільшення кількості псевдовузлів дозволить порушити механізми маршрутизації, агрегації даних, розподіленого зберігання даних тощо.

Механізми захисту: криптографія з відкритим ключем, цифрові підписи, автентифікація.

*Воронка (Sinkhole attack).*Скомпрометований вузол підмінює метрики маршрутизації та діє як базова станція з метою концентрації на собі якомога більше трафіку в певному сегменті мережі. Це призводить до розділення мережі, втрати пакетів, виснаження ресурсів і призупинення служб маршрутизації всієї мережі (рис. 2).

Механізми захисту: автентифікація та шифрування даних, захищена маршрутизація, система виявлення вторгнень, випадковий вибір маршрутів.

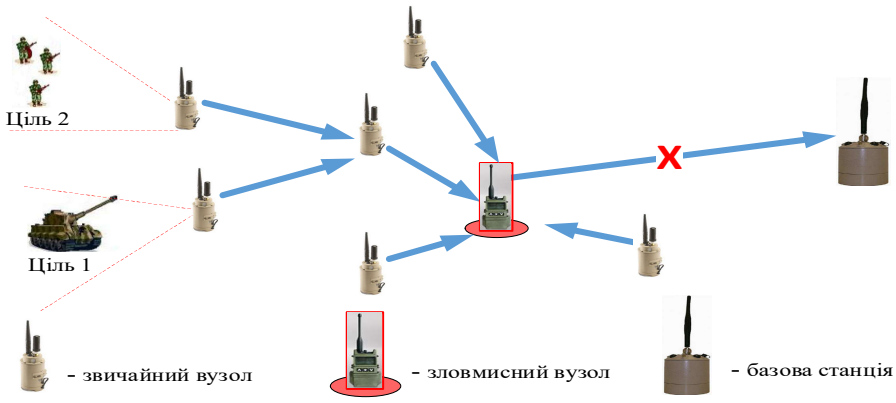

Рисунок 2 – Атака воронки

Hello флуд атака (HELLO flood attack). Трансляція зловмисником пакетів HELLO за допомогою потужного передавача для визначення іншими вузлами його як найближчого сусіда в мережі [16].

Механізми захисту: шифрування пакетів і автентифікація вузлів, обмеження кількості хопів для Hello пакетів.

Вибіркова передача (Selective Forwarding). Створений зловмисником вузол може вибірково видаляти певні вхідні пакети та/або надавати високий пріоритет власним повідомленням.

Механізми захисту: багатошляхова маршрутизація, випадковий вибір маршрутів, перевірка доставки пакетів.

Атака чорної діри (Black Hole attack). Скомпрометований вузол змінює метрики маршрутизації, щоб змусити сусідні вузли пересилати всі повідомлення через нього. Весь вхідний мережевий трафік на цьому вузлі буде знищенно.

Механізми захисту: багатошляхова

маршрутизація, система довіри сусідніх вузлів, система виявлення вторгнень.

Тунелювання (Wormhole attack). Створення зловмисником тунелю для передачі повідомлень між двома вузлами різних сегментів мережі за рахунок зменшення метрик у маршрутних повідомленнях. За таких умов вузли вважають себе сусідами (рис. 3).

Механізми захисту: багатошляхова маршрутизація, система довіри сусідніх вузлів.

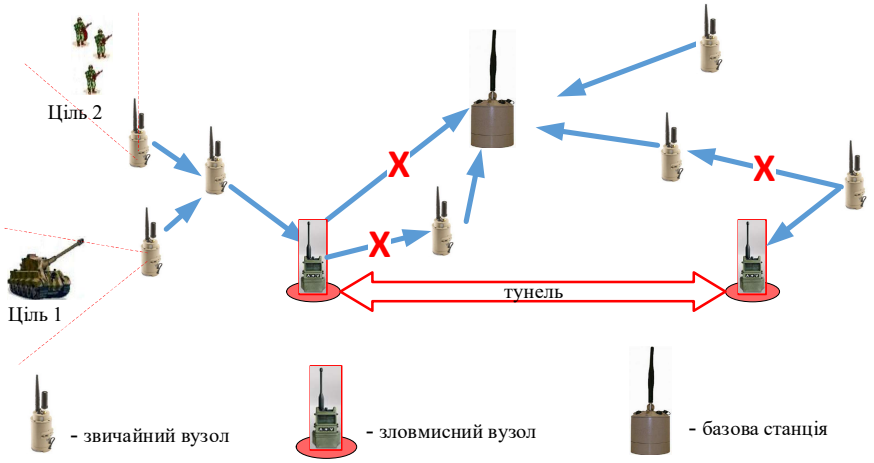

Рисунок 3 – Атака тунелювання

Модифікація маршрутної інформації (Spoofed Routing Information). Скомпрометовані вузли порушують обмін маршрутною інформацією між іншими вузлами, що призводить до появи петель маршрутизації, збільшення вихідних мережевих маршрутів, збільшення часу затримки та появи фальшивих повідомлень про помилки.

Механізми захисту: лічильники часових позначок, шифрування й автентифікації даних, захищена маршрутизація, система виявлення вторгнень.

Визначення топології мережі (Homing). Аналіз зловмисником широкомовних повідомлень (зондів-запитів) з метою виявлення маршрутів, вузлів, шлюзів та станцій мережі.

Механізми захисту: шифрування даних і заголовків пакетів, маскування.

Затоплення (Flooding). Зловмисний вузол постійно надсилає багато запитів для встановлення з'єднання з іншими вузами, що призводить до виснаження їх ресурсів.

Механізми захисту: обмеження на кількість з'єднань та швидкості передачі, система виявлення вторгнень.

Десинхронізація (Desynchronization attack). Надсилання шкідливих пакетів, змушує вузли відправляти пакети в неправильному порядку або в невідповідних часових інтервалах.

Механізми захисту: автентифікація та шифрування даних, система виявлення вторгнень.

Перенавантаження (Overwhelm attack). Одночасне надсилання великої кількісті запитів або пакетів до одного або декількох вузлів з метою зниження якості обслуговування (QoS) всієї ЮБСМ [17].

Механізми захисту: система виявлення вторгнень, захищена агрегація даних, обмеження швидкості передачі

DoS-атака на маршрутизацію (Path-based DoS attack) Надсилання скомпрометованими вузлами надмірної кількісті пакетів на конкретний маршрут (шлях) для зниження якості обслуговування на ньому.

Механізми захисту: багатошляхова маршрутизація, випадковий вибір маршрутів, система виявлення вторгнень [18].

Шкідливе програмне забезпечення (Malware attack). Впровадження шкідливого коду(вірусів, хробаків, троянів) в один або декілька вузлів мережі з метою їх перепрограмування для реалізації майбутніх атак.

Механізми захисту: система виявлення вторгнень, оновлення програмного забезпечення створення резервної конфігурації мережі.

Моніторинг та прослуховування (Monitoring and Eavesdropping) спостереження за функціонуванням мережі та обміном інформації в ній для перехоплення конференційної інформації.

Механізми захисту: шифрування даних, обфускація трафіку.

Аналіз трафіку (Traffic Analysis) проведення зловмисниками аналізу патернів або метаданих перехопленого мережевого трафіку.

Механізми захисту: шифрування метаданих, обфускація трафіку, випадковий вибір маршрутів.

Таким чином за ознаками, наведеними у класифікації (рис. 1) описано атаки на БСМ та розглянуто механізми захисту від них.

Висновки й перспективи подальших досліджень

На основі проведеного аналізу існуючих вразливостей для забезпечення безпеки безпроводових сенсорних мереж тактичної ланки управління військами удосконалено класифікацію атак на мобільні мережі за додатковою ознакою стосовно об'єктів системи управління. Такий підхід дає змогу розподілити атаки на підсистеми управління моніторингом, топологією,

маршрутизацією, енергоресурсу вузлів, радіоресурсом, якістю обслуговування безпроводових сенсорних мереж.

Згідно із запропонованою класифікацією найбільшу загрозу становлять атаки, що можуть бути реалізовані на мережевому і транспортному рівні моделі взаємозв'язку відкритої системи OSI й спрямовані на порушення доступності та виснаження ресурсів безпроводових сенсорних мереж. Також слід урахувати, що пасивні атаки пов'язані з моніторингом, прослуховуванням та аналізом трафіку не впливають на наведені в класифікації підсистеми системи управління безпроводових сенсорних мереж тактичної ланки управління військами.

Основними напрямами подальшого дослідження є розроблення архітектури побудови (функціональної моделі) підсистеми управління безпекою з урахуванням особливостей характеристик, методів побудови та організації безпроводових сенсорних мереж.

Список бібліографічних посилань

1. 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, №2. С. 96–112. **2. Міночкін А. І., Романюк В. А., Жук О. В.** Перспективи розвитку тактичних сенсорних мереж. *Збірник наукових праць ВІТІ НТУУ «КПІ»*. 2007. №2. С. 112–119. **3. Міночкін А. І., Романюк В. А.** Безпека мобільних радіомереж. *Збірник наукових праць ВІТІ НТУУ «КПІ»*. 2004. № 5. С. 116–26. **4. Міночкін А. І., Романюк В. А., Шаціло П. В.** Виявлення атак в мобільних радіомереж. *Збірник наукових праць. ВІТІ НТУУ «КПІ»*. 2005. № 1. С. 102–111. **5. Amine Kardi. Rachid Zagrouba**. Attacks classification and security mechanisms in Wireless Sensor Networks. Advances in Science, Technology and Engineering Systems Journal. 2019. Vol. 4. № 6. P. 229–243. **6. Tomić I. et McCann Ju. A.** A Survey of Potential Security Issues in Existing Wireless Sensor Network Protocols. *IEEE Internet of Things Journal*. 2017. Vol. 4. № 6. P. 1910–1923. **7. Sharifnejad M., Sharifi M., Ghiasabadi M. and Beheshti S.** A survey on Wireless Sensor Networks Security. *4th International Conference: sciences of Electronic, Technologies of Information and Telecommunications*, March 25–29, 2007. TUNISIA. **8. Bhavana B., Kumar Sh. P. and Silakari S.** An Exhaustive Survey on Physical Node Capture Attack in WSN. *International Journal of Computer Applications.* 2014. № 95.3. **9. Rakesh Kumar S., Ritika R. et Sandip V.** Data Flow in Wireless Sensor Network Protocol Stack by using Bellman-Ford Routing Algorithm. *Bulletin of Electrical Engineering and Informatics*. 2017. Vol. 6. № 1. P. 81–87. **10. Shyamala R. et Valli Sh.** Impact of DoS Attack in Software Defined Network for Virtual Network. *Wireless Personal Communications*. 2017. Vol. 94. № 4. P. 2189–2202. **11. Akshat T., Juhi K. et Monica Bh.** Threats to security of Wireless Sensor Networks. In: *Cloud Computing, Data Science & Engineering-Confluence*. 2017 7th International Conference on. IEEE. 2017. P. 402–405. **12. Duru C., Aniedu A., Innocent O. T. & Ekene A.** Modeling of wireless sensor networks jamming attack strategies. *Am. Sci. Res. J. Eng. Technol.* 2020. Sci. № 67. P. 48–65. **13. Jia Z., Yulong Z. et Baoyu Z.** Physical-Layer Security and Reliability Challenges for Industrial Wireless Sensor Networks. *IEEE Access*. 2017. **14. Dinker A. G. et Sharma V.** Attacks and challenges in wireless sensor networks. In : *Computing for Sustainable Global Development (INDIACom),* 2016 3rd International Conference on. IEEE. 2016. P. 3069–3074. **15. Newaz Sh. Shah, Cuevas Á., Lee G. M et al.** Improving energy saving in time-division multiplexing passive optical networks. *IEEE Internet Computing*. 2013. Vol. 17. № 1. P. 23–31. **16. Singh V. P., Ukey A S. A. et Jain S**. Signa lstrength based hello flood attack detection and prevention in wireless sensor networks. *International Journal of Computer Applications*. 2013. Vol. 62. № 15. **17. Garcia-Font V., Garrigues C. et Rifà-Pous H**. Attack Classification Schema for Smart City WSNs. Sensors. 2017. Vol. 17. № 4. P. 771. **18. Shi L., Liu Q., Shao J., Cheng Y.** Distributed localization in wireless sensor networks under denial-of-service attacks. *IEEE Control Syst. Lett*. 2021. № 5 (2). P. 493–498

CLASSIFICATION OF ATTACKS IN WIRELESS SENSOR NETWORKS OF THE TACTICAL COMMAND AND CONTROL OF TROOPS

Artiukh Serhii [1]
Zhuk Oleksandr *(Doctor of Technical Sciences, Associate Professor)* [2]
Cherneha Volodymyr *(Candidate of Technical Science, Associate Professor)* [2]

[1] *Military institute of telecommunications and information technologies named after Heroes of Kruty, Kyiv, Ukraine*
[2] *National Defence University of Ukraine, Kyiv, Ukraine*

Formulation of the problem in general. *Today, wireless sensor networks are actively used for reconnaissance and surveillance, rapid collection of information about the enemy, which is transmitted to control centers for analysis and decision-making in real time. Solving the issues of information security in the use of sensors comes to the fore during combat operations. The purpose of the article is to analyze existing vulnerabilities and improve the classification of attacks in wireless sensor networks of the tactical command and control of troops to ensure their security. In writing the article, theoretical methods were applied, namely, analysis of research and publications on the development and implementation of wireless sensor networks in the military sphere, analysis of existing attacks on such networks and synthesis of the classification of attacks on wireless sensor networks of the tactical command and control of troops. This methodological approach makes it possible to develop methods of countering attacks and improve the mechanisms for protecting wireless sensor networks of the tactical command and control.*

Analysis of recent researches and publications *Today, the security of Mobile Ad-Hoc Networks (MANETs) is being actively studied, their main vulnerabilities are identified, existing attacks are classified and threats are assessed, and mechanisms for ensuring the security of these networks are analyzed. However, the vulnerabilities and attacks on wireless sensor networks are not fully considered, and their peculiarities of operation and security issues are not taken into account. The author also proposes a classification of attacks in wireless sensor networks by four features, but does not take into account the specifics of the use of such networks in the tactical command and control of troops.*

Presenting the main material *The paper analyzes the vulnerabilities determined by the peculiarities of the architecture of wireless sensor networks and their functioning protocols. The basic and additional security requirements for such networks are described. An improved classification of attacks in wireless sensor networks is presented based on the following features: the nature of actions, the level of the open systems model, the purpose of the impact, the object of control, positioning relative to the network, and the type of attacking device. Based on the proposed classification, the existing attacks in wireless sensor networks of the tactical command and control of troops are analyzed. The novelty of the work is that the classification of attacks on mobile radio networks has been improved by violation of confidentiality, integrity, availability, authentication, and resource depletion. For the first time, a classification of attacks is proposed based on the impact on various objects of the control system (control subsystems for monitoring, topology, routing, node energy, radio resource, and quality of service). In accordance with the proposed classification, the essence of attacks on wireless sensor networks of the tactical command and control of troops is revealed and mechanisms for protecting against them are proposed.*

Elements of scientific novelty*. The analyzed vulnerabilities and the presented classification contribute to the deepening of scientific knowledge about the security of control systems for wireless sensor networks of the tactical command and control of troops.*

Practical significance of the article. *The applied use of attack classification features will contribute to the construction of a modern intrusion detection system as a security management subsystem for wireless sensor networks of the tactical command and control of troops, designed to increase the effectiveness of countering attacks on these networks and ensure the required level of security compliance.*

Conclusion and the perspectives of future researches. *To ensure the security of wireless sensor networks of the tactical command and control of troops, the classification of attacks on mobile networks has been improved by an additional feature regarding the objects of the control system. The main directions for further research are the development of an architecture (functional model) of the security management subsystem, taking into account the peculiarities of the characteristics, methods of construction and organization of wireless sensor networks.*

Keywords: *tactical control link, automated information system, wireless sensor networks, heterogeneous information sources, sensor nodes, unmanned aerial vehicles, vulnerability, attack classification, control system objects, protection mechanism.*

References

1. Mashtalir, V. V., Zhuk, O. V., Minenko, L. M., Artiukh, S. G., (2023). Conceptual approaches to the use of wireless sensor networks by the armies of the world's leading countries. Modern Information Technologies in the Sphere of Security and Defence. 2, 96-112. **3. Zhuk, O. V., Minochkin, A. I., Romaniuk, V. A.,** (2007). Prospects for the Development of Tactical Sensor Networks. *Collection of Scientific Works of VITI NTUU «KPI»*, 2, 112-119. **3. Minochkin, A. I., Romaniuk, V. A.,** (2004). Mobile Radio Network Security. *Collection of Scientific Works of VITI NTUU «KPI»*. 2, 116-126. **4. Minochkin, A. I., Romaniuk, V. A., Shatsilo, P. V.,** (2005). Detecting attacks on mobile radio networks. *Collection of Scientific Works of VITI NTUU «KPI»*. 1, 102-111. **5. Amine Kardi. Rachid Zagrouba,** (2019). Attacks classification and security mechanisms in Wireless Sensor Networks. *Advances in Science, Technology and Engineering Systems Journal.* 4, 6, 229-243. **6. Tomić, Ivana et McCann, Julie A.,** (2017). A Survey of Potential Security Issues in Existing Wireless Sensor Network Protocols. *IEEE Internet of Things Journal*, 4, 6, 1910-1923. **7. Mona Sharifnejad, Mohsen Sharifi, Mansoureh Ghiasabadi and Sareh Beheshti**, (2007). A survey on Wireless Sensor Networks Security, 4th International Conference: sciences of Electronic, Technologies of Information and Telecommunications, March 25-29, 2007, TUNISIA. **8. Butani, Bhavana, Piyush Kumar Shukla, and Sanjay Silakari**, (2014). An Exhaustive Survey on Physical Node Capture Attack in WSN. *International Journal of Computer Applications*. 95.3. **9. Saini, Rakesh Kumar, RITIKA, Ritika, et Vijay, Sandip,** (2017). Data Flow in Wireless Sensor Network Protocol Stack by using Bellman-Ford Routing Algorithm. *Bulletin of Electrical Engineering and Informatics*, 6, 1, 81-87. **10. Ramachandran, Shyamala et Shanmugam, Valli,** (2017). Impact of DoS Attack in Software Defined Network for Virtual Network. *Wireless Personal Communications*, 94, 4, 2189-2202. **11. Tyagi, Akshat, Kushwah, Juhi, et Bhalla, Monica,** (2017). Threats to security of Wireless Sensor Networks. In: *Cloud Computing, Data Science & Engineering-Confluence, 2017 7th International Conference on. IEEE,* 402-405. **12. Duru C., Aniedu A., Innocent O. T., & Ekene A.,** (2020). Modeling of wireless sensor networks jamming attack strategies. Am. Sci. Res. J. Eng. Technol. Sci, 67, 48-65. **13. Zhu, Jia, Zou, Yulong, et Zheng, Baoyu,** (2017). Physical-Layer Security and Reliability Challenges for Industrial Wireless Sensor Networks. *IEEE Access*. **14. Dinker, Aarti Gautam et Sharma, Vidushi,** (2016). Attacks and challenges in wireless sensor networks. In : Computing for Sustainable Global Development (INDIA Com), *3rd International Conference on. IEEE*, 3069-3074. **15. Newaz, Sh Shah, Cuevas, Ángel, Lee, Gyu Myoung, et al.,** (2013). Improving energy saving in time-division multiplexing passive optical networks. *IEEE Internet Computing*. 17, 1, 23-31. **16. Singh, Virendra Pal, Ukey, Aishwarya S. Anand, et Jain, Sweta,** (2013). Signa lstrength based hello flood attack detection and prevention in wireless sensor networks. *International Journal of Computer Applications*, 62, 15. **17. Garcia-Font, Victor, Garrigues, Carles, et Rifà-Pous, Helena,** (2017). Attack Classification Schema for Smart City WSNs. *Sensors*, 17, 4, 771. **18. Shi, L., Liu, Q., Shao, J., Cheng, Y.,** (2021). Distributed localization in wireless sensor networks under denial-of-service attacks, *IEEE Control Syst. Lett*. 5 (2), 493–498.