УДК 621.382 (045)

АНАЛІЗ ЗАГРОЗ ТА МЕХАНІЗМІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СЕНСОРНИХ МЕРЕЖАХ

Олександр Корченко, Марек Алєксандер, Роман Одарченко, Абду Наджі, Олена Петренко

В роботі проаналізовані особливості та перспективи розвитку сучасних безпроводових сенсорних мереж. Розглянуті найбільш популярні стандарти, які використовуються для їх побудови. Наведені основні вимоги до пристроїв, що складають архітектуру сучасних безпроводових сенсорних мереж, зокрема, висока енергоефективність, портативність, автономність. Було розглянуто основні види існуючих мережевих протоколів, що використовуються у сенсорних мережах у відповідності до еталонної моделі взаємодії відкритих систем, зокрема, фізичного, канального, мережевого, транспортного та прикладного рівнів, з огляду на проблеми забезпечення інформаційної безпеки. Було визначено проблемні місця систем захисту та систематизовано класифікацію різних типів атак на сенсорні мережі. Показано, що основні цілі забезпечення інформаційної безпеки в безпроводових сенсорних мережах можна умовно розділити на першочергові (забезпечення конфіденційності, цілісності, аутентифікації і доступності даних) і другорядні (свіжість даних, самоорганізація, часова синхронізація, захищена локалізація). Це в свою чергу дало змогу запропонувати розширену класифікацію механізмів забезпечення безпеки в них, що дозволяє мінімізувати потенційні збитки від різних типів атак.

Ключові слова: *бездротова сенсорна мережа; протокол; технологія ZigBee; трафік; стандарт IEEE 802.15.4; маршрутизація.*

Вступ. Безпроводові сенсорні мережі стають як новим важливим рівнем в IT екосистемі, так і об'єктом жвавих досліджень, що включають апаратну і програмну архітектуру, мережеві технології та з'єднання, розподілені алгоритми, програмні моделі, управління даними, безпеку і т.д. В загальному розумінні сенсорна мережа – це безліч маленьких зчитувальних пристроїв (датчиків), здатних реєструвати зміни різних параметрів навколишнього середовища і транслювати ці параметри іншим подібним пристроям, що знаходяться в зоні досяжності, з певною метою, наприклад: відеоспостереження, моніторинг навколишнього середовища тощо [16] (рис. 1).

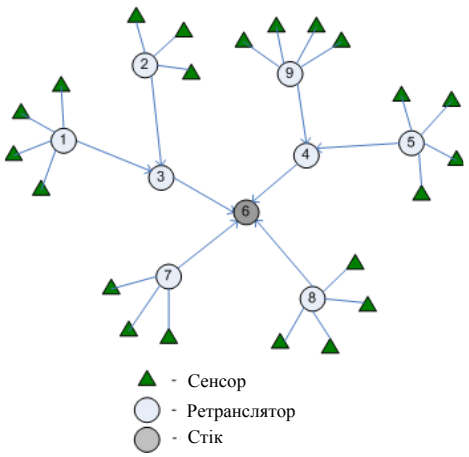

Рис. 1. Типова структура сенсорної мережі

Серед основних цілей використання сенсорних мереж можна виділити наступні.

1) Системи безпеки – контроль периметрів, визначення вторгнення, віддалене спостереження; моніторинг персоналу, охорона цінностей та творів мистецтва, домашні системи безпеки, системи пожежної сигналізації.

2) Системи моніторингу і контролю навколишнього середовища (вологість, температура, склад повітря / ґрунту / води, тиск, магнітний фон); моніторинг забруднення навколишнього середовища, міграція тварин, комах.

3) Системи електроенергії – управління енергопостачанням; контроль кондиціонування, вентиляції, опалення, освітлення; ретранслятори для лічильників газу, води, електроенергії.

4) Надзвичайні ситуації – оповіщення про стихійні лиха: лісові пожежі, зсуви і т. п;. порятунок людей при надзвичайних ситуаціях.

Тому, як бачимо, досить часто сенсорні мережі можуть розгортатися в агресивних несприятливих середовищах, де можуть бути зроблені навмисні спроби впливу на їх роботу. Яскравим прикладом може слугувати їх застосування в зоні бойових дій, де таємність переданих даних і розташування, а також стійкість до спроб компрометації даних і знищення мережі, мають ключове значення.

Аналіз існуючих досліджень та публікацій. Питання функціонування існуючих протоколів в безпроводових мережах розглядаються багатьма вченими [3, 5]. Проблемою забезпечення енергоефективності сенсорних мереж вирішувалися в [7]. Дослідженням безпроводових сенсорних мереж в системах охоронної сигналізації займалися в роботах [13-15]. Типи та вплив різних типів атак на сенсорні мережі досліджували в [9, 11, 12, 16]. Стандартні методи захисту у мережах ZigBee наведено в[4, 5].

Постановка завдання. Проте в проаналізованих джерелах не наведено уніфікованої класифікації загроз та методів захисту від них в сучасних сенсорних мережах. Тому досліджені джерела [9, 11, 12, 16] вимагають систематизації знань про типи атак та способи захисту від них у сенсорних мережах. Це дозволяє сформувати мету дослідження, яка полягає в аналізі та систематизації загроз у сенсорних мережах; визначенні механізмів захисту від них.

Поставлена мета передбачає вирішення наступних задач:

1. Дослідження протоколів, які використовуються в сенсорних мережах та їх недоліків обміну інформацією з точки зору забезпечення інформаційної безпеки.

2. Систематизація можливих типів атак на сенсорні мережі.

3. Дослідження механізмів забезпечення безпеки в сенсорних мережах.

Виклад основного матеріалу дослідження. В загальному випадку кожний пристрій оснащений мікроконтролером, прийомопередавачем, елементом живлення і набором датчиків для вимірювання деяких параметрів навколишнього середовища, наприклад, температури, освітленості, вібрації, тиску, рівня шуму та інших (рис. 2) [1].

Інтелектуальні вузли такої мережі здатні ретранслювати повідомлення один від одного по черзі, забезпечуючи значну площу покриття системи при малій потужності передавачів. За рахунок цього досягається висока енергетична ефективність системи. Нижче розглянемо протоколи, які використовуються в сучасних сенсорних мережах.

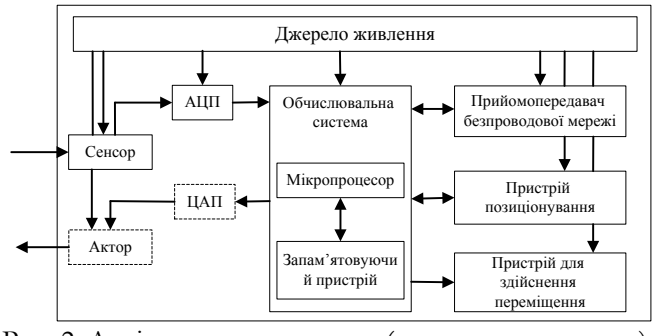

Рис. 2. Архітектура сенсорного (сенсорно-акторного) вузла. Обов'язкові елементи виділені безперервної лінією, необов'язкові – переривчастою

Протоколи фізичного рівня. До протоколів фізичного рівня для безпроводової сенсорної мережі (БСМ) застосовуються ті ж обмеження, що і до протоколів інших рівнів, а саме: невеликий запас електроенергії, маленькі габарити і вартість сенсорного вузла. З даних обмежень безпосередньо випливає, що протокол фізичного рівня повинен забезпечувати мінімально ресурсомісткі алгоритми модуляції і демодуляції, а також забезпечувати невелику площу радіопокриття, так як потужність радіопередавача в умовах обмеженого запасу електроенергії безпосередньо впливає на час життя сенсорного вузла: чим більше потужність передавального пристрою, тим швидше вичерпається автономне джерело електроживлення.

Серед відкритих протоколів для фізичного рівня загальноприйнятим для побудови БСМ є стандарт IEEE 802.15.4, що визначає крім фізичного рівня для низькошвидкісних персональних безпроводових мереж (Wireless Personal Area Networks, WPAN) ще і частину канального рівня – рівеня доступу до середовища (Medium Access Control, MAC) [2, 7].

Остання версія стандарту IEEE 802.15.4 описує шість різних типів організації фізичного рівня (не враховуючи регіональних типів, призначених для Китаю і Японії і описуваних в IEEE 802.15.4c і IEEE 802.15.4d відповідно), які представляють собою поєднання використання зазначених частотних смуг із застосуванням різних типів модуляції сигналу: двійкової фазової маніпуляції, квадратурної фазової маніпуляції, комбінації двійкової фазової маніпуляції і амплітудної маніпуляції, широкосмугової технології UWB і методу лінійної частотної модуляції (Chirp Spread Spectrum, CSS).

Найбільш перспективним для побудови БСМ є використання широкосмугових технологій, які входять в стандарт IEEE 802.15.4 останньої редакції, так як вони дозволяють створювати прийомопередавачі з низьким енергоспоживанням. Цю тезу також підтверджує велика кількість досліджень даної технології, виконаних за останні роки [3-6].

Базова відстань передачі сигналу для IEEE 802.15.4 – 10 метрів, що єцілком достатньою для БСМ. Максимальна швидкість передачі даних складає 250кбіт/с.

Протоколи канального рівня. Канальний рівень, відповідно до концепції IEEE 802, можна розділити на два підрівні, що виконують різні функції. Більш низький підрівень доступу до середовища або MAC-рівень виконує функції розмежування і розпізнавання кадрів, адресації в рамках одного середовища доступу, а також розмежування доступу до середовища передачі, в тому числі уникнення, виявлення та вирішення колізій. Верхній підрівень управління логічним зв'язком (Logical link control, LLC) займається мультиплексуванням і демультиплексуванням потоків даних, встанов-

ленням з'єднань між вузлами в рамках одного середовища передачі, в деяких випадках – контролем коректності переданих кадрів та виправленням помилок.

Вимоги до протоколів канального рівня БСМ можна сформулювати наступним чином: дані протоколи повинні бути енергетично економічними, повинні давати можливість швидко встановлювати з'єднання між будь-якими двома вузлами, що мають доступ до одного і того ж середовища (так як БСМ є ad hoc, а не інфраструктурними мережами), і забезпечувати можливість самоорганізації великого числа вузлів. Також слід зазначити, що реалізація таких протоколів не повинна вимагати великих обчислювальних ресурсів.

Для організації MAC-рівня БСМ також досить часто використовується стандарт IEEE 802.15.4. Він реалізує всі необхідні функції даного рівня з невеликими витратами електроенергії. Розмежування доступу до середовища передавання реалізується за допомогою методу множинного доступу з контролем несучої і униканням колізій (Carrier Sense Multiple Access With Collision Avoidance, CSMA/CA).

Стандарт IEEE 802.15.1 є набагато більш економічним і з цієї точки зору цілком підходить для організації БСМ. Але даний стандарт має ряд інших обмежень. Так, Bluetooth, що розроблявся спочатку для того, щоб обмін інформацією між пристроями проводився не за допомогою проводів, а через бездротовий інтерфейс, має дуже великий (близько 5 секунд) час встановлення з'єднання, що робить його невпридатним для БСМ, в яких необхідно мати можливість, наприклад, швидкого переконфігурування мережі. До того ж об'єднання в одну мережу більше 8 Bluetooth-пристроїв вимагає з'єднання декількох пікомереж, що також створює деякі складності при реалізації БСМ з використанням даної технології.

Протоколи мережевого рівня і протоколи маршрутизації. Протоколи мережевого рівня БСМ, крім стандартних вимог до енергетичної ефективності та використання невеликих обчислювальних потужностей, також мають низку додаткових вимог, пов'язаних зі специфікою БСМ. Це, в першу чергу, підтримка режиму багатоітеральної (multihop) передачі даних. Також протоколи мережевого рівня повинні забезпечувати підтримку самоорганізації мережі. Крім того, при проектуванні протоколів мережевого рівня БСМ зазвичай враховується, що дані в таких мережах передаються здебільшого в напрямку від сенсорних вузлів до шлюзу БСМ.

Протоколи транспортного рівня. Оскільки протоколи транспортного рівня призначені для доставки даних, в тому числі між мережами, для БСМ, що представляють собою окрему мережу, в складних і інтелектуальних протоколах даного рівня найчастіше немає необхідності, оскільки будь-який протокол вимагає для своєї роботи додаткових апаратних ресурсів і електроживлення, які в сенсорних вузлах можуть бути дуже обмежені.

У той же час, з урахуванням розвитку протоколу 6LoWPAN, а також концепції IP, видається цілком розумним використання в БСМ транспортних протоколів, широко застосовуваних у мережі Інтернет, для забезпечення доступу до сенсорних вузлів з глобальної мережі. І якщо використання протоколу контролю передачі (Transmission Control Protocol, TCP) може бути не зовсім виправдано з урахуванням великого розміру заголовку (від 20 байт) і відносної складності реалізації, які можуть вимагати неприйнятно великих для БСМ ресурсів, то протокол призначений для передачі дейтаграм користувача (User Datagram Protocol , UDP), хоч і не забезпечує гарантованої доставки, цілком може застосовуватися в БСМ у зв'язку з більшою, ніж для TCP, простотою реалізації і меншим розміром заголовку (8 байт).

Протоколи верхніх рівнів. Необхідно зауважити, що протоколи верхніх рівнів, зокрема, прикладного рівня для БСМ, значною мірою залежать від того, для яких саме цілей буде використовуватися сенсорна мережа. Оскільки зараз вже існує достатньо велика кількість додатків для БСМ, і ще більша кількість додатків знаходиться на стадії розробки, зараз досить складно виділити якісь загальновизнані і широко використовувані відкриті протоколи верхніх рівнів для БСМ.

Але в той же час на ринку вже існує кілька компаній, які реалізували різні протоколи верхніх рівнів для БСМ і успішно експлуатують свої розробки.

Найбільш відомим з таких компаній є альянс ZigBee [8], який створив протокол мережевого рівня для роботи поверх IEEE 802.15.4 і ряд протоколів прикладного рівня, призначених для автоматизації будівель і житла, охорони здоров'я, економії електроенергії та ін. Параметри технології ZigBee наведені в табл. 1.

Таблиця 1

Параметри технології ZigBee

Параметр	Значення параметру
Тип топології мережі	Повна mesh-мережа
Відстань між вузлами, м	70
Швидкість обміну даними, кбіт/с	250
Максимальна кількість вузлів	65520
Робочий діапазон частот, ГГц	2,4 (16 каналів)
Можливості енергозберігання	Неповні (перехід в режим очікування дозволений тільки кінцевим вузлам)
Складність	Висока (128 кбіт флеш-пам'яті)
Вартість	Низька
Надійність	Добра
Самовідновлення	Так
Стандартизація	Так
Взаємодія з іншими пристроями	Так

Основні напрямки забезпечення інформаційної безпеки в безпроводових сенсорних мережах. Основні цілі забезпечення інформаційної безпеки в БСМ можна умовно розділити на першочергові і другорядні. Першочергові цілі широко відомі і включають в себе забезпечення конфіденційності, цілісності, аутентифікації і доступності даних. Другорядні цілі забезпечення безпеки включають в себе такі поняття як «свіжість» даних, самоорганізація, часова синхронізація, захищена локалізація.

Атаки на безпроводові сенсорні мережі. Більшість загроз інформаційній безпеці в безпроводових мережах схожі з загрозами і атаками на проводові мережі, за винятком того, що безпроводові мережі важче захистити внаслідок використання відкритого середовища в якості носія даних і широкомовної природи безпроводових з'єднань (рис. 3). Нижче розглянемо основні мережеві атаки в БСМ.

Пасивні атаки. Аналіз трафіку і прослуховування комунікаційного каналу неавторизованими особами класифікується як пасивна атака. Атаки, націлені виключно на отримання даних, що передаються є пасивними по своїй природі. Найбільш частими є наступні види атак, спрямовані на порушення конфіденційності даних:

1) *Моніторинг і прослуховування*. Даний вид атаки зустрічається найбільш часто. За допомогою підслуховування зловмисник може з легкістю отримати доступ до даних, що передаються. При передачі контрольної інформації про конфігурацію мережі, дана техніка може становити найбільшу небезпеку для конфіденційності даних.

2) *Аналіз трафіку*. Навіть коли інформація передається в зашифрованому вигляді, залишається ймовірність використання зловмисником техніки аналізу комунікаційних патернів. Активність сенсорів потенційно може розкрити досить інформації для нанесення зловмисником шкоди сенсорній мережі.

Рис. 3. Класифікація атак на БСМ

Активні атаки. Різні модифікації даних під час комунікації, що здійснюються авторизованими особами, класифікуються як активні атаки. Нижче надведено характеристики активних атак.

Атаки маршрутизації. Атаки, які здійснюються на мережевому рівні (network layer) моделі OSI називаються атаками маршрутизації. Наступні атаки маршрутизації зустрічаються найбільш часто:

Змінена маршрутна інформація. До впливу даної атаки найбільш схильні децентралізовані мережі, де кожен вузол є маршрутизатором і відповідно може змінювати маршрутну інформацію. Внаслідок даної атаки може відбуватися створення кільцевого маршруту, збільшуватися час доставки пакету даних до точки призначення і т.д.

Вибіркова розсилка. Скомпрометований вузол сенсорної мережі може вибірково видаляти певні пакети. Особливо ефективною дана атака може бути в

комбінації з атаками, які збирають велику кількість трафіку на даному вузлі мережі. В результаті даної атаки серйозно страждає цілісність і доступність даних, що може істотно знизити рівень якості надання сервісу сенсорною мережею [9].

Атака Воронки (Sinkhole Attack). Дана атака характерна тим, що скомпрометований вузол мережі починає діяти по типу воронки, збираючи весь трафік сенсорної мережі [10]. Особливо в мережах з протоколом маршрутизації, заснованому на широкомовній розсилці, зловмисник прослуховує запити на маршрутну інформацію і відповідає сенсорним вузлам, що «знає» найкоротший маршрут до базової станції. Як тільки скомпрометованому вузлу вдалося стати між транслюючим сенсорним вузлом і базовою станцією, він може виконувати будь-які дії з пакетам даних, що надходили.

Атака Sybil attack. Під час даної атаки один скомпрометований вузол може використовувати кілька псевдоідентифікаторів, видаючи себе відразу за кілька вузлів. Подібні атаки використовуються для порушення механізму розподіленого зберігання, механізмів маршрутизації, механізмів агрегації даних, механізмів голосування в мережі і т. д. По суті будь-яка мережа з рівноправними вузлами (особливо безпроводові і децентралізовані мережі) є схильними до даної атаки.

Атака Wormhole attack. Дана атака передбачає створення спеціального шляху між двома і більше скомпрометованими вузлами сенсорної мережі для передачі по ним перехоплених пакетів, доступних тільки для атакуючої системи [11]. Подібні атаки представляють серйозну загрозу безпеці сенсорної мережі тому, що не вимагають компрометації вузла сенсорної мережі. Тоді, коли вузол В (базова станція або звичайний вузол) використовує трансляцію розсилки для запиту маршруту, зловмисник отримує даний запит і перенаправляє його до найближчого сусіда. Будь-який вузол, який отримав подібний перенаправлений запит розглядає себе як вузол, що знаходиться в зоні досяжності вузла В і запам'ятовує вузол В, як свого «батька». Навіть, якщо цей вузол знаходиться на великій відстані від вузла В і його відокремлюють від вузла В безліч сенсорних вузлів, він буде розглядати вузол В як найближчий від себе.

Флуд атака (HELLO flood attack). Дана атака є широкомовною атакою, яка служить для того, щоб передати в сенсорну мережу масу необов'язкових повідомлень, які повинні позбавити мережу різноманітних ресурсів – канальної ємності, обчислювальної потужності, енергетичних ресурсів і т.д. Під час подібної атаки зловмисник за допомогою високочастотного радіопередавача з достатньою обчислювальною потужністю розсилає Hello пакети безлічі вузлів сенсорної мережі. Вузли, які отримали Hello пакети, розглядають скомпрометований вузол як свого сусіда. Під час наступної передачі даних, вони будуть використовувати отриману адресу з Hello пакетів для відправки. Таким чином, зловмисник отримає доступ до даних.

Відмова в обслуговуванні. Даний вид атаки може бути результатом умисного виведення з ладу вузлів сенсорної мережі або ж результатом дій зловмисників. Найпростіша атака такого роду спрямована на витрату всіх ресурсів, доступних скомпрометованому вузлу за допомогою відправки непотрібних пакетів даних, таким чином перешкоджаючи легітимним користувачам мережі отримувати призначені їм сервіси і ресурси [12]. Дана атака означає не тільки спроби зловмисника зруйнувати мережу або розірвати з'єднання, але і будь-яку подія, що знижує здатність мережі надавати певні послуги і ресурси. Безліч типів подібних атак може бути здійснено на різних рівнях моделі OSI, які до цього були розглянуті.

Захоплення вузла (node subversion). Захоплення вузла зловмисником може спричинити розкриття важливої інформації, наприклад, криптографічних ключів, що в свою чергу може спричинити компрометацію всієї сенсорної мережі [13].

Несправність вузла (malfunction). Несправний в результаті атаки вузол генерує невірні дані, що може порушити цілісність сенсорної мережі, особливо, якщо несправний вузол є вузлом, який агрегує дані, наприклад, головним вузлом кластера [13].

Простій вузла / вихід з ладу. Простій вузла або його вихід з ладу трапляється тоді, коли вузол перестає функціонувати. У разі виходу з ладу головного вузла кластера, протокол сенсорної мережі повинен бути здатним надати альтернативний маршрут для доставки пакетів даних.

Фізичні атаки. Вузли сенсорної мережі часто встановлюються в середовищах із зовнішніми впливами. В таких середовищах маленький формфактор вузлів сенсорної мережі в поєднанні з відсутністю постійного нагляду за ними робить їх схильними до різних фізичних атак. На відміну від інших видів атак, фізичні атаки руйнують сенсори незворотньо.

Спотворення повідомлення. Будь-яка зміна контенту повідомлення зловмисником неминуче компрометує цілісність даних, що передаються [14].

Хибний вузол. Даний вид атак передбачає впровадження в мережу вузла, який надсилає вузлам сенсорної мережі некоректні дані. Дана атака є однією з найбільш небезпечних атак, оскільки вузол, який поширює зловмисний код, може привести до зупинки всієї сенсорної мережі [14].

Копіювання вузла мережі. Концептуально дана атака полягає в наступному: зловмисник намагається додати заздалегідь підготовлені вузли в існуючу сенсорну мережу, використовуючи ідентифікатори вже існуючих вузлів в ній. Для цього зловмисник фізично захоплює один вузол мережі з метою отримання його унікальних даних. Отримані дані згодом використовуються для конфігурації заздалегідь підготовлених вузлів, які згодом стають клонами захопленого вузла. За допомогою впровадження реплікованих вузлів в певні точки мережевої топології зловмисник може з легкістю управляти сегментом мережі.

Механізми забезпечення безпеки. Механізми забезпечення безпеки використовуються для ідентифікації, запобігання і відновлення після атак. Механізми забезпечення безпеки можна умовно розділити на механізми високого і низького рівня. Рис. 4 ілюструє класифікацію механізмів забезпечення безпеки.

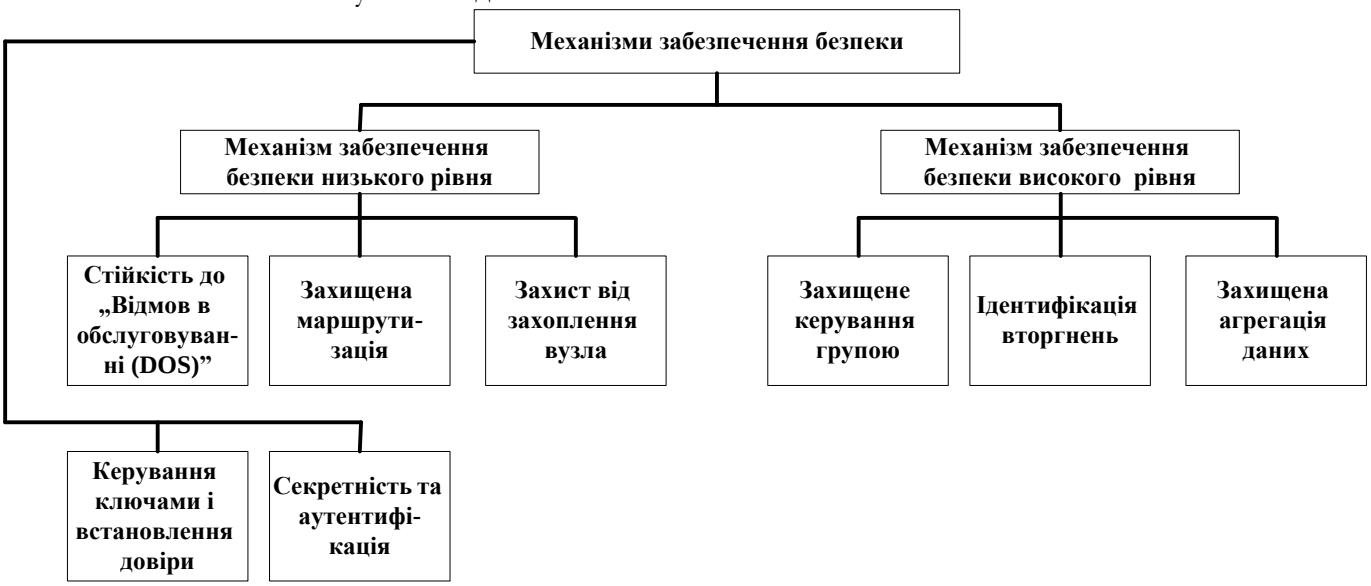

Рис. 4. Механізми забезпечення безпеки

Механізми забезпечення безпеки низького рівня. *Управління ключами і встановлення довіри.* Через лімітовані ресурси, особливо ресурси енергетичної батареї, асиметричне шифрування ключами не повинно використовуватися для сенсорних мереж. Таким чином, необхідно використовувати симетричне шифрування. Техніки встановлення і управління ключами повинні бути придатними для використання в мережах з сотнями і тисячами вузлів. Крім того, комунікаційні патерни сенсорних мереж відрізняються від традиційних аналогів, вузли сенсорної мережі повинні встановлювати ключі з їх сусідами і з вузлами, що агрегують інформацію. Недолік цього методу полягає в тому, що зловмисники, скомпрометувавши велику кількість вузлів мережі, можуть відновити весь пул ключів і розшифрувати дані [15].

Секретність і аутентифікація. Сенсорні мережі вимагають захисту від прослуховування, ін'єкцій і модифікації пакетів. Криптографія є стандартним захистом. Складнощі виникають в процесі застосування криптографії для сенсорних мереж. У мережах з рівноправними вузлами, криптографія з міжкінцевим шифруванням (end to end cryptography) дозволяє досягти високого рівня безпеки, проте вимагає встановлення ключів між усіма вузлами мережі і є несумісною з широкомовною розсилкою і пасивною участю (технологія, завдяки якій вузол, що прослуховує сусідній до нього вузол мережі може вирішити не передавати дані, в разі якщо точно такі дані передаються сусіднім вузлом). Криптографія на канальному рівні спрощує установку ключів і підтримує пасивну участь і широкомовній розсилці, проте дозволяє проміжним вузлам перехоплювати і змінювати повідомлення.

Стійкість до відмов в обслуговуванні (DOS). Причинами відмови в обслуговуванні можуть бути проблеми апаратного забезпечення, помилки в програмному забезпеченні, недостатність ресурсів, несприятливі умови зовнішнього середовища або сукупність впливу вище перерахованих факторів. Наприклад, зловмисник може спробувати вивести сенсорну мережу з ладу за допомогою передачі потужного сигналу, який здатний повністю заглушити всі комунікації вузлів сенсорної мережі. Технологія розширення спектру використовується для захисту сенсорних мереж від подібних атак. Вона передбачає використання методів навмисного розширення діапазону частот сигналу. Діапазон частот стає більшим, ніж необхідно для передачі повідомлення. Передача такого сигналу схожа на шум, що дозволяє знизити ризики навмисного інтерференційного впливу на інформаційний сигнал з боку зловмисників.

Захищена маршрутизація. Маршрутизація є ключовим процесом, без якого неможливо здійснювати комунікацію між вузлами сенсорної ме-

режі. Однак сучасні протоколи маршрутизації містять безліч вразливостей інформаційної безпеки. Найпростіші атаки можуть мати на меті впровадження скомпрометованої маршрутної інформації в сенсорну мережу, що згодом створює проблеми в передачі даних від відправника в кінцеву точку призначення. Розробка нових схем аутентифікації і захищених протоколів маршрутизації може захистити мережі від подібних атак.

Захист від захоплення вузла. Захоплення вузла є серйозною проблемою для захисту даних в сенсорних мережах. Часто сенсорні мережі встановлюються в легкодоступних для зловмисників місцях. Зловмисник, захопивши вузол мережі, може дістати криптографічну інформацію, перепрограмувати вузол мережі або замінити вилучений вузол зловмисними вузлами. Найбільш поширеними методами захисту є використання захищеної від злому упаковки, алгоритмічних рішень, техніки хешування тощо.

Механізми забезпечення безпеки високого рівня. *Захищене управління групою.* Кожен вузол бездротової сенсорної мережі обмежений в обчислювальних ресурсах і комунікаційних можливостях. Однак, такі функції як агрегацію мережевих даних і їх аналіз може здійснювати група вузлів сенсорної мережі. Наприклад, група сенсорів мережі може виконувати спільне стеження за пересуванням певного об'єкта. Вузли сенсорної мережі в групі можуть постійно і швидко змінюватися. Внаслідок цього, необхідні захищені протоколи для управління групами вузлів сенсорної мережі, які повинні дозволяти захищене прийняття вузлів в функціональні групи і підтримувати захищені комунікації вузлів-членів функціональних груп.

Ідентифікація вторгнень. Безпроводові сенсорні мережі схильні до різних вторгнень. Основне завдання механізмів ідентифікації вторгнень полягає в моніторингу сенсорної мережі, ідентифікації можливих спроб проникнення і розсилки відповідних повідомлень користувачам. Для децентралізованих механізмів ідентифікації вторгнень може бути перспективним підходом використання технології захищених груп [15].

Захищена агрегація даних. Дані, які збираються з вузлів сенсорної мережі, потім часто агрегуються на рівні базової станції. Завдяки агрегації даних за допомогою сенсорної мережі можна розрахувати середню температуру в географічному регіоні, комбінувати дані сенсорних вузлів для розрахунку місця розташування і швидкості транспортного засобу і т. д. Точки агрегації даних схильні до різних видів атак і повинні бути надійно захищені. Скомпрометовані вузли можуть бути використані для впровадження помилкових даних, які згодом призведуть до неправильних агрегованих розрахунків. Захищені протоколи маршрутизації і схеми аутентифікації корисні для запобігання впровадження помилкових даних в сенсорну мережу.

Висновки. Низка специфічних вимог до пристроїв, що стосуються низького споживання енергії, невеликої вартості, простоти розгортання і самоорганізації вузлів, призвів до створення в останні роки окремого напрямку розвитку мереж зв'язку – БСМ. Перспективи їх поширення очевидно дуже великі. Тому в даний час представляється вкрай актуальним всебічне дослідження різних аспектів функціонування БСМ, а також створення адекватних моделей надходження трафіку від окремих сенсорних вузлів і БСМ в цілому, захист інформації в БСМ.

У даній роботі було проаналізовано протоколи, які використовуються в сенсорних мережах та визначено їх недоліки з точки зору забезпечення інформаційної безпеки; систематизовано можливі типи атак на сенсорні мережі та запропоновані механізми забезпечення безпеки в сенсорних мережах, що дозволяють значно мінімізувати загрози інформаційній безпеці БСМ.

Майбутні дослідження мають на меті виявлення недоліків БСМ з точки зору забезпечення конфіденційності цілісності та доступності в архітектурі «клієнт-сервер-шлюз-вузол», дослідження протоколів захисту, їх недоліків та можливих шляхів удосконалення.

ЛІТЕРАТУРА

[1]. Dunkels, A. Distributed TCP caching for wireless sensor networks / A. Dunkels, J.Alonso , T.Voigt , and H.Ritter // In Proceedings of the 3rd AnnualMediterranean Ad Hoc Networking Workshop (MedHoc-Net). - 2004.

[2]. Xiang, L. Design Of Household Control System Based On ZigBee, GSM and TCP/IP Protocol / L. Xiang // 10th IEEE International Conference on Control and Automation (ICCA). - 2013. - 1372-1375 pp.

[3]. 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.

[4]. Akl, A. An investigation of self-organization in wireless sensor networks / A. Akl, T.Gayraud , and P.Berthou // IEEE International Conference on Networking, Sensing and Control (ICNSC). - 2001. - 1-6 pp.

[5]. 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.

[6]. "IEEE 802.15.4a: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)" – Institute of Electrical and Electronics Engineers, 2007

[7]. Баскаков С. С. Исследование способов повышения эффективности маршрутизации по виртуальным координатам в беспроводных сенсорных сетях // Вестник МГТУ им. Баумана. Сер. Приборостроение. 2009. № 2. С. 112–124.
[8]. ZigBee Alliance [Электронный ресурс] URL: http://www.zigbee.org/
[9]. Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", AdHoc Networks (elsevier), Page: 299 – 302, year 2003.
[10]. Culpepper B.J., Tseng H.C. Sinkhole intrusion indicators in DSR MANETs // Proc. First International Conference on Broad band Networks. 2004. – Pp. 681–688.
[11]. Hu Y., C. Perrig, Johson D.B. Packet leashes: a defense against wormhole attacks in wireless networks // Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies, – Voume 3. – 3 April 2003. – Pp. 1976–1986.
[12]. Blackert W.J., Gregg D.M., Castner A.K., Kyle E.M., Hom R.L., and Jokerst R.M. Analyzing interaction between distributed denial of service attacks and mitigation technologies // Proc. DARPA Information Survivability Conference and Exposition, – Volume 1. – 24 April, – 2003. – Pp. 26–36.
[13]. Pathan A.S.K.; Hyung-Woo Lee; Choong Seon Hong, "Security in wireless sensor networks: issues and challenges" Advanced Communication echnology (ICACT), Page(s):6, 2006.
[14]. Zia T.; Zomaya A., "Security Issues in Wireless Sensor Networks", Systems and Networks Communications (ICSNC) Page(s): 40 – 40 , year 2006.
[15]. Adrian Perrig, John Stankovic, David Wagner, "Security in Wireless Sensor Networks" Communications of the ACM, Page 53 – 57, year 2004.
[16]. [Электронный ресурс] URL: http://sibac.info/studconf/tech/xxxii/42203
[17]. 802.15.4 IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs). Published by The Institute of Electrical and Electronics Engineers, Inc. 3 Park Avenue, New York, NY 10016-5997, USA.
[18]. Скуснов А.. ZigBee: взгляд вглубь // Компоненты и технологи. – 2005. – № 4.

REFERENCES

[1]. Dunkels, A. Distributed TCP caching for wireless sensor networks / A. Dunkels, J.Alonso , T.Voigt , and H.Ritter // In Proceedings of the 3rd AnnualMediterranean Ad Hoc Networking Workshop (MedHoc-Net). - 2004.
[2]. Xiang, L. Design Of Household Control System Based On ZigBee, GSM and TCP/IP Protocol / L. Xiang // 10th IEEE International Conference on Control and Automation (ICCA). – 2013. – 1372-1375 pp.
[3]. 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.
[4]. Akl, A. An investigation of self-organization in wireless sensor networks / A. Akl, T.Gayraud , and P.Berthou // IEEE International Conference on Networking, Sensing and Control (ICNSC). – 2001. – 1-6 pp.
[5]. 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. – N 5. – 16–27 pp.
[6]. "IEEE 802.15.4a: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)" – Institute of Electrical and Electronics Engineers, 2007
[7]. Baskakov S.S. Research ways to improve routing efficiency for virtual coordinates in wireless sensor networks // Vestnik MSTU. Bauman. Ser. Instrument. 2009. № 2. S. 112-124.
[8]. ZigBee Alliance [electronic resource] URL: http://www.zigbee.org/
[9]. Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", AdHoc Networks (elsevier), Page: 299 – 302, year 2003.
[10]. Culpepper B.J., Tseng H.C. Sinkhole intrusion indicators in DSR MANETs // Proc. First International Conference on Broad band Networks. 2004. – Pp. 681 – 688.
[11]. Hu Y., C. Perrig, Johson D.B. Packet leashes: a defense against wormhole attacks in wireless networks // Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies, - Voume 3. – 3 April 2003. – Pp. 1976 – 1986.
[12]. Blackert W.J., Gregg D.M., Castner A.K., Kyle E.M., Hom R.L., and Jokerst R.M. Analyzing interaction between distributed denial of service attacks and mitigation technologies // Proc. DARPA Information Survivability Conference and Exposition, - Vol. 1. – 2003. – Pp. 26 – 36.
[13]. Pathan A.S.K.; Hyung-Woo Lee; Choong Seon Hong, "Security in wireless sensor networks: issues and challenges" Advanced Communication echnology (ICACT), Page(s):6, 2006.
[14]. Zia T.; Zomaya A., "Security Issues in Wireless Sensor Networks", Systems and Networks Communications (ICSNC) Page(s):40 – 40, 2006.

[15]. Adrian Perrig, John Stankovic, David Wagner, "Security in Wireless Sensor Networks" Communications of the ACM, Page 53 – 57, 2004.
[16]. [Electronic resource] URL: http://sibac.info/studconf/tech/xxxii/42203
[17]. 802.15.4 IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs). Published by The Institute of Electrical and Electronics Engineers, Inc. 3 Park Avenue, New York, NY 10016-5997, USA.
[18]. Skusnov A. ZigBee: look deep into // Components and technologies. - 2005. - № 4.

ИССЛЕДОВАНИЯ И КЛАССИФИКАЦИЯ МЕХАНИЗМОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЕНСОРНЫХ СЕТЯХ

В работе проанализированы особенности и перспективы развития современных беспроводных сенсорных сетей. Рассмотрены наиболее популярные стандарты, которые используются для их построения. Приведены основные требования к устройствам, составляющим архитектуру современных беспроводных сенсорных сетей, в частности, высокая энергоэффективность, портативность, автономность. Были рассмотрены основные виды существующих сетевых протоколов, используемых в сенсорных сетях в соответствии с эталонной моделью взаимодействия открытых систем, в частности, физического, канального, сетевого, транспортного и прикладного уровней, учитывая проблемы обеспечения информационной безопасности. Были определены проблемные места систем защиты и систематизировано классификацию различных типов атак на сенсорные сети. Показано, что основные цели обеспечения информационной безопасности в беспроводных сенсорных сетях можно условно разделить на первоочередные (обеспечение конфиденциальности, целостности, аутентификации и доступности данных) и второстепенные (свежесть данных, самоорганизация, временная синхронизация, защищена локализация). Это в свою очередь дало возможность предложить расширенную классификацию механизмов обеспечения безопасности в них, что позволяет минимизировать потенциальные убытки от различных типов атак.

Ключевые слова: беспроводная сенсорная сеть; протокол; технология ZigBee; трафик; стандарт IEEE 802.15.4; маршрутизация .

RESEARCH AND CLASSIFICATION OF INFORMATION SECURITY MECHANISMS IN SENSOR NETWORKS

The paper analyzed the modern wireless sensor networks characteristics and prospects of development. Considered the most popular standards used for their construction. The basic requirements for the devices that make up the modern architecture of wireless sensor networks, including high energy efficiency, portability, autonomy, ware shown. It was considered the basic types of existing network protocols used in sensor networks according to the reference open systems interconnection model, including physical, data link, network, transport and application levels, related the problems of information security. Were identified problem areas of protection and classification systematically various types of attacks in sensor networks. It is shown that the main objectives of information security in wireless sensor networks can be divided into primary (confidentiality, integrity, authentication and data availability) and minor (fresh data, self-organization, time synchronization, localization protected). This in turn has provided an opportunity to offer enhanced security classification mechanisms in them, which minimizes potential damage from various types of attacks.

Index Terms: wireless sensor network, protocol, ZigBee technology, IEEE 802.15.4 standard, routing

Корченко Олександр Григорович, доктор технічних наук, професор, завідувач кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: icaocentre@nau.edu.ua
Корченко Александр Григорьевич, доктор техниче-ских наук, профессор, заведующий кафедрой безопасности информационных технологий Национального авиационного университета.
Korchenko Alexander, Professor, Doctor of Science in Eng., Head of IT-Security Academic Department, National Aviation University (Ukraine).

Алєксандер Марек Богуслав, кандидат технічних наук, докторант Національного авіаційного університету, доцент Державної вищої технічної школи у Новому Сончі (Польща).
E-mail: aleksandermarek4@gmail.com
Александер Марек Богуслав, кандидат технических наук, докторант Национального авиационного университета, доцент Государственной высшей технической школы в Новом Сонче (Польша).
Aleksander Marek Buguslav, Ph.D., doctorate candidate in National Aviation University, Associate Professor in State Higher Vocational School in Nowy Sacz (Poland).

Одарченко Роман Сергійович, кандидат технічних наук, доцент кафедри телекомунікаційних систем Національного авіаційного університету.
E-mail: odarchenko.r.s@mail.ru
Одарченко Роман Сергеевич, кандидат технических наук, доцент кафедры телекоммуникационных систем Национального авиационного университета.
Odarchenko Roman, Ph.D., Associate Professor in Telecommunication Academic Systems Dept of National Aviation University.

Наджі Абду Ахмад Алі, здобувач кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: abdonagi@hotmail.com
Наджи Абду Ахмад Али, соискатель кафедры безопасности информационных технологий Национального авиационного университета.
Nagi Abdu Ahmad Ali, external PhD student in IT-Security Academic Dept of National Aviation University. E-mail:

Петренко Олена Юріївна, студент кафедри телекомунікаційних систем Національного авіаційного університету.
E-mail: aferist008@ramler.ru
Петренко Елена Юрьевна, студент кафедры телекоммуникационных систем Национального авиационного университета.
Petrenko Elena, student in Telecommunication Systems Academic Dept of National Aviation University.