УДК 621.382

# КЕРІВНІ ПРИНЦИПИ ТА ПІДХОДИ ДО ЗАХИСТУ ІНФОРМАЦІЇ У БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖАХ

**Туранська О. С., Петрова В.М.**
*Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна*
*E-mail: turanska.o.s@gmail.com*

**Guiding principles and approaches to information security in Wireless Sensor Networks**

Wireless sensor networks (WSN) have many applications in our time. For example in military, rescue works and other areas. WSN have many sensors which can be located in hostile territory. If we want save confidential information, we mustensure information security when it is transmitted over the network. That's why we need to know Guiding principles and approaches to information security.

Питання забезпечення захисту інформації в безпроводових сенсорних мережах(БСМ) є дуже важливим. Це пояснюється тим, що на сьогоднішній день БСМ мають безліч застосувань у військовій, внутрішній безпеці та інших областях.Безпека в таких випадках має важливе значення, оскільки безпроводові сенсорні мережі часто розгортаються на ворожій території і можуть мати важливе стратегічне значення. Атаки на таку мережу можуть призвести до витоку конфіденційної інформації. Крім того, безпроводовий зв'язок, який використовується мережами датчиків, полегшує підслуховування і отримання інформації противником.

Комбінація цих факторів вимагає впровадження заходів безпеки для сенсорних мереж під час проектування, щоб забезпечити надійність роботи та конфіденційність даних у сенсорних середовищах.

Основними керівними принципами захисту інформації в безпроводових сенсорних мережах є:

1. Безпека мережі визначається безпекою всіх шарів.
2. У масово розподіленій мережі, заходи безпеки повинні бути піддані динамічній реконфігурації та децентралізованому управлінню.
3. В даній мережі в будь-який момент часу витрати, пов'язані з заходами безпеки, не повинні перевищувати витрати, які були вирахувані з врахуванням ризиків.
4. Якщо фізична безпека вузлів у мережі не гарантується, заходи безпеки повинні бути стійкими до фізичного втручання з вузлами в області експлуатації.
5. Через різноманітність обмежень у БСМ, при розробці схеми безпеки слід уважно розглянути наступні аспекти: енергоефективність, щільність вузла та надійність, адаптивність, самостійна конфігурація, простота та

локальний ідентифікатор.

Впровадження заходів для забезпечення захисту інформації в безпроводових сенсорних мережах ускладнюється особливостями самих мереж, такими як: датчики чутливі до фізичного захоплення, датчики з безпроводовим зв’язком легко підслуховувати, в таку мережу зловмисник може легко внести шкідливе повідомлення, технології захисту від стискання та фізичної витримки неможливі через велику конструктивну складність та споживання енергії, обмеження датчиків роблять безпроводову сенсорну мережу більш сприйнятливими до атаки відмови в обслуговуванні, мала місткість пам’яті унеможливлює втілити централізоване технології набору ключових слівіснує конфлікт між споживанням ресурсів та максимізацією рівня безпеки, при цьому необхідно забезпечували максимально низьку загальну вартість БСМ.

Для досягнення безпеки в БСМ  важливо мати можливість виконувати різні криптографічні операції, включаючи шифрування, автентифікацію тощо.Проте рішення щодо вибору відповідного методу криптографії залежить від обчислень та можливостей зв'язку вузлів датчиків. Асиметрична криптографія часто є надто дорогою для багатьох застосувань. Тим не менш, симетрична криптографія не така універсальна, як криптографічні методи публічного ключа, що ускладнює розробку захищених програм. Застосування будь-якої схеми шифрування вимагає передачі додаткових бітів, отже, додаткової обробки, пам'яті та заряду акумулятора, що є дуже важливими ресурсами для довговічності датчиків.Застосування механізмів безпеки, таких як шифрування, також може збільшити затримку, джиттер і втрати пакетів в БСМ.

Захист криптографічної системи залежить, головним чином, від секретності ключа, який в ній використовує. Схеми керування ключами - це механізми, що використовуються для встановлення та розповсюдження в мережі різноманітних криптографічних ключів, таких як окремі клавіші, парні клавіші та групові ключі.Ключове управління - це важливий криптографічний примітив, на якому будуються інші примітиви безпеки. Якщо зловмисник може знайти ключ, вся система зламається.

Ще одним підходом, який використовується для підвищення безпеки при роботі БСМ, є збереження агрегації даних.

Агрегування даних - це процес, в якому проміжні вузли, які називаються «агрегаторами», збирають первинну інформацію з датчиків, обробляють її локально і відправляють тільки результат кінцевому користувачеві.Ця важлива операція істотно зменшує в мережі кількість даних, що передаються, і, таким чином збільшує час життя датчиків. При цьому даний процес може бути уразливим до атак і потребує ефективного захисту даних, що передаються.

Першою лінією захисту даних від загроз та атак є криптографічні механізми: цілісність і конфіденційність можуть бути досягнуті з

використанням криптографічних схем.

Проблемою такого методу є необхідність гарантувати те, що користувач все ще може бути впевнений в точності агрегованих даних, навіть якщо агрегатор і невелике підмножина вузлів датчика знаходяться під контролем противника. У захищених протоколах агрегування даних потрібно порівняння продуктивності з точки зору таких матриць, як безпека, накладні витрати на обробку даних, накладні витрати на зв'язок, споживання енергії і ступінь стиснення даних.

Для вирішення цієї проблеми необхідно розробити нові протоколи агрегації даних, щоб забезпечити більш високу масштабованість і надійність від обману агрегатора і вузла датчика. Забезпечити криптографію всередині внутрішньої обробки даних (захищена обробка даних), безпечні, дуже ефективні і економічні механізми агрегації даних, достовірність і надійність агрегованих даних. Також необхідна безпечна схема агрегації даних в середовищах без великих вузлів.

Внутрішня обробка необроблених даних виконується в безпроводових сенсорних мережах шляхом ділення мережі на невеликі групи і аналізу даних, агрегованих у лідерів групи.

Тому лідер групи повинен аутентифікувати дані, які він отримує від інших вузлів в групі.Для цього потрібно керувати ключовими ключами. Однак додавання або видалення вузлів з групи призводить до більшої кількості проблем.

Отже, потрібні безпечні протоколи для групового управління.

Проблеми безпеки є потенційним каменем спотикання для майбутнього широкого розгортання сенсорних мереж. БСМ все ще знаходяться в процесі розробки, і багато протоколів, розроблені до цього часу для БСМ, не враховують безпеку.З іншого боку, істотні особливості безпроводових сенсорних мереж роблять дуже складною розробку сильних протоколів безпеки при збереженні низьких накладних витрат.

Багато проблем безпеки в БСМ залишаються відкритими, проте розуміння особливостей роботи та керівних принципів забезпечення захисту інформації дозволяє нам знаходити нові підходи до вирішення цієї проблеми.

## Література


1. Chris Karlof and David Wagner, “Secure routing in wireless sensor networks: attacks and countermeasures”, Ad Hoc Networks, Elsevier Publications, 2003.
2. T.Kavitha and D.Sridharan, “Security Vulnerabilities In Wireless Sensor Networks: A Survey”, Journal of Information Assurance and Security (2010), 2010.
3. Murat Dener, “Security Analysis in Wireless Sensor Networks”, year 2014.
4. Половко А.М., Гуров С. В. Основитеоріїнадійності. – СПб.: БХВ-Петербург 2006. – 560 с.