УДК 621.396

МЕТОДИ ПІДВИЩЕННЯ БЕЗПЕКИ В БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖАХ

Афанасьєв Я.Р., Новіков В.І.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: afanassiev.yaroslav@gmail.com

Methods to Improve Security in Wireless Sensor Network

Currently, wireless sensor networks (BSN) are one of the most promising areas in the development of telecommunications system. The wireless sensor network (BSN) is a technology, which is a self-organizing network of a large number of sensors and devices that are connected to each other via a radio channel. Security and privacy are of great importance in wireless sensor networks, where the unique characteristics of these networks and the purpose of the application they use make them attractive targets for penetration and other attacks.

Безпроводові сенсорні мережі (БСМ) є новим важливим етапом розвитку телекомунікаційних систем. Основу безпроводової сенсорної мережі складають безліч маленьких зчитувальних пристроїв (датчиків), здатних реєструвати зміни різних параметрів навколишнього середовища і транслювати ці параметри іншим подібним пристроям. Сучасні датчики здатні відстежувати тиск, температуру, вологість, склад ґрунту, автомобільний рух, рівні шуму, наявність або відсутність певних об'єктів або речовин та інші. В безпроводових сенсорних мережах спілкуються не тільки один з одним, але і з базовою станцією (БС), через безпровідні канали, що дозволяє їм надавати зібрані дані для віддаленої обробки, візуалізації, аналізу та зберігання. В таких системах виникають проблеми, пов'язані з інформаційною безпекою.

Основні проблеми з якими зустрічаються при використання ефективної схеми безпеки в БСМ пов'язані з розмірами датчиків, обчислювальною потужністю, пам'яттю і типами розв'язуваних завдань, очікуваних від датчиків. Для вирішення основних питань з приводу безпеки в безпроводових сенсорних мережах необхідно застосовувати криптографію та стеганографію. Також доцільно розглянути різні типи загроз і нападів на безпроводові сенсорні мережі.

Безпека була проблемою в обчислювальних системах і мережах протягом декількох десятиліть, під час яких типи атак, і заходи безпеки, і механізми, що протистоять їм, удосконалилися і значно розвинулися, особливо через швидке зростання Інтернету. Мета забезпечення інформаційної безпеки в безпроводових сенсорних мережах можна умовно розділити на основні і другорядні. Основні цілі включають в себе забезпечення конфіденційності, цілісності, аутентифікації і доступності даних. Другорядні цілі забезпечення безпеки включають в себе такі поняття як свіжість даних, самоорганізація, тимчасова синхронізація, захищена локалізація. Розглянемо основні цілі:

1.Конфіденційність даних є фундаментальним завданням безпеки. Дані, зібрані сенсорами, можуть містити конфіденційну інформацію і не повинні

бути пропущені до несанкціонованих пристроїв. Також інформація про самі сенсори (наприклад місце розташування, і т.д.), повинні бути захищені, щоб запобігти підслуховуванню і атакам. Ці проблеми вимагають заходів, які забезпечують конфіденційність даних для сенсорних мереж.

2.Цілісність даних в сенсорних мережах визначається здатністю забезпечення захисту даних таким чином, щоб дані не могли змінитись під час транспортування між вузлами сенсорної мережі.

3.Аутентифікація необхідна для підтвердження ідентифікації користувача або пристрою, гарантуючи, що повідомлення прибуло від того, хто стверджує, що його послав.

4.Цілісність даних в сенсорних мережах визначається здатністю забезпечення захисту даних таким способом, щоб дані не могли бути змінені під час транспортування між вузлами сенсорної мережі, наприклад, з метою введення помилкових даних і отже впливу на сенсорні дані.

У всіх типах мережі зв'язку є кілька фундаментальних механізмів безпеки, які можуть бути використані, щоб забезпечити конфіденційність, цілісність і доступність. Щоб захиститися від багатьох можливих атак можна використовувати безліч протоколів захисту та інші захисні механізми. Для цього використовуються криптографічні та стеганографічні методи. Криптографія - процес приховування і захисту інформації, використовуючи кодування і декодування. Підходи криптографії симетричного ключа можуть бути значно ефективнішими з точки зору ресурсів, що робить їх кращим вибором в БСМ. Головний недолік підходу симетричного ключа - проблема ключового розподілу, тобто спільно використовуваний симетричний ключ повинен спочатку бути відомий обом зв'язувальним вузлам, перш ніж вони зможуть надійно обмінюватися даними.

У той час як криптографія спрямована на приховування змісту повідомлення, стеганографія спрямована на приховування існування повідомлення. Вона приховує існування каналу, і, крім того, в тому випадку, якщо ми хочемо відправити секретні дані без інформації про відправника або коли ми хочемо поширювати секретні дані публічно, вона дуже корисна. Однак, безпеку безпроводових сенсорних мереж не має прямого відношення до стеганографії, а для обробки мультимедійних даних (наприклад, аудіо, відео) гостро не вистачає ресурсів, це є відкритою на даний момент проблемою БСС.

Фізичний рівень безпечного доступу до безпроводових сенсорних мереж може бути забезпечений використанням стрибкоподібної перебудови частоти. Динамічне поєднання таких параметрів, як доступні частоти для стрибкоподібної перебудови, час затримки в перебудові і шаблон стрибкоподібної перебудови може бути використано з малою витратою пам'яті, обробкою і енергетичними затратами.

Також для вирішення проблем безпеки розроблені спеціальні протоколи, найбільшу популярність серед яких має технологія ZigBee. В основі даної технології лежить стандарт IEEE 802.15.4, який описує фізичний рівень і рівень доступу до середовища для безпроводових сенсорних мереж передачі даних. Стандарт IEEE 802.15.4 забезпечує чотири основні моделі безпеки: управління

доступом, цілісність повідомлення, конфіденційність повідомлення і захист відтворення. Безпека в IEEE 802.15.4 оброблена рівнем MAC, і програма може вибрати певні вимоги до захисту, встановивши належні параметри. Стандарт розрізняє вісім наборів безпеки (розглянуті в таблиці 1), кожен з різними рівнями захисту для переданих даних.

Назва	Опис
Null	Не надає захисту
AES – CTR	Надає тільки шифрування, CTR
AES – CBC – MAC – 128	128-bit MAC
AES – CBC – MAC – 64	64-bit MAC
AES – CBC – MAC – 32	32-bit MAC
AES – CCM – 128	Шифрування і 128-bit MAC
AES – CCM – 64	Шифрування і 64-bit MAC
AES – CCM – 32	Шифрування і 32-bit MAC

Таблиця.1 Набори безпеки які підтримані в IEEE 802.15.4.

Окрім до засобів захисту IEEE 802.15.4 специфікація ZigBee також представляє поняття центру довіри, відповідальність зазвичай прийнята на координатора ZigBee. Центр довіри відповідальний за аутентифікацію пристроїв, що бажають приєднатися до мережі (адміністратор довіри), підтримка і розподіл ключів (адміністратор мережі) і включення безпеки між пристроями (менеджер конфігурації).

Безпроводові мережі застосовуються в багатьох сферах людської діяльності, тому питання безпеки грає важливу роль. Як і будь-яка комп'ютерна мережа, бездротові сенсорні мережі піддаються безлічі загроз і атак, як більшість інших мереж, сенсорні мережі вимагають підтримки конфіденційності, цілісності і аутентифікації для захисту сенсорних вузлів і сенсорних даних. Запропоновані методи підвищення безпеки в БСМ, методи і протоколи захисту мережі можуть забезпечити необхідний рівень безпеки безпроводових сенсорних мереж.

Література

1. John Paul Walters, Zhengqiang Liang, Weisong Shi, Vipin Chaudhary, “Wireless Sensor Network Security: A Survey”, Security in Distributed, Grid and Pervasive Computing Yang Xiao (Eds), Page3-5, 10—15, year 2006.
2. Adrian Perrig, John Stankovic, David Wagner, “Security in Wireless Sensor Networks” Communications of the ACM, Page 53—57, year 2004.
3. 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, year 2006.
4. Zia T.; Zomaya A., “Security Issues in Wireless Sensor Networks”, Systems and Networks Communications (ICSNC) Page(s):40—40, year 2006.