УДК 004.056.5:343.326
DOI: 10.31673/2409-7292.2020.033943

Боярчук Р.М., Пуха М.С., Маковський А.П., Айстраханов К.Д., Філін М.Ю.

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЗВ'ЯЗКУ В БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖАХ НА ОСНОВІ БАГАТОРІВНЕВОЇ АРХІТЕКТУРИ ЗАХИСТУ

Мережі безпроводових мікросенсорів, які використовуються для моніторингу фізичного середовища, стали важливою областю застосування безпроводових технологій. Ключовими атрибутами цих нових типів мережевих систем є суворо обмежені обчислювальні та енергетичні ресурси, а також спеціальне робоче середовище. Ця стаття є дослідженням аспектів комунікаційної безпеки цих мереж. Обмеження ресурсів та специфічна архітектура сенсорних мереж вимагають індивідуальних механізмів безпеки. Наш підхід полягає у класифікації типів даних, що існують у сенсорних мережах, та виявленні можливих загроз безпеці зв'язку відповідно до цієї класифікації. Ми пропонуємо схему захисту зв'язку, де для кожного типу даних ми визначаємо відповідний механізм захисту. Застосовуючи цю багаторівневу архітектуру безпеки, де кожен механізм має різні вимоги до ресурсів, ми забезпечуємо ефективне управління ресурсами, що є важливим для безпроводових сенсорних мереж.

Ключові слова: безпроводова сенсорна мережа, датчик, зв'язок, захист.

Вступ

Безпроводові сенсорні мережі, що застосовуються для моніторингу фізичного середовища, стали важливим додатком, який є результатом поєднання безпроводового зв'язку та вбудованих обчислювальних технологій [1]. Сенсорні мережі складаються з сотні або тисячі вузлів – пристроїв малої потужності, оснащених одним або декількома датчиками [2] (Рис. 1). Окрім датчиків, вузол, як правило, містить схеми обробки сигналів, мікроконтролери та безпроводовий передавач/приймач. Подаючи інформацію про фізичний світ в існуючу інформаційну інфраструктуру, очікується, що ці мережі приведуть у майбутнє, де обчислювальні роботи тісно поєднані з фізичним світом і навіть використовуються для впливу на фізичний світ за допомогою виконавчих механізмів. Такі системи включають моніторинг віддалених місць, відстеження цілей на полі бою, створення мережі допомоги при стихійних лихах, раннє виявлення пожеж у лісах та моніторинг навколишнього середовища.

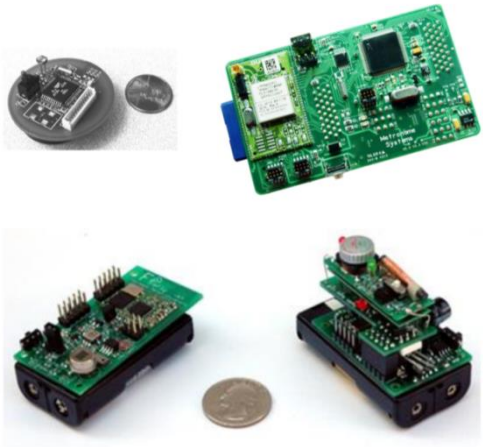

Рис. 1. Обладнання сенсорних мереж

Аналіз літературних джерел

Дослідження сенсорних мереж зосереджувались переважно на енергоефективності [3], мережевих протоколах [4] та розподілених базах даних. При цьому безпеці комунікацій приділяється набагато менше уваги [5]. Однак у багатьох випадках аспекти безпеки настільки ж важливі, як продуктивність та низьке споживання енергії. Окрім систем на полі бою, безпека має вирішальне значення для безпеки приміщень та спостереження, а також при застосуванні датчиків у таких критичних системах, як аеропорти, лікарні тощо.

Постановка завдання дослідження

Сенсорні мережі мають відмінні риси, найважливішими з яких є обмежені енергетичні та обчислювальні ресурси. Для урахування цих відмінностей для сенсорних мереж повинні бути адаптовані існуючі або створені нові механізми безпеки.

Виклад основного матеріалу

Зловмисний мобільний код, введений у мережу може змінити поведінку мережі непередбачуваними способами: 1) Застосовуючи датчики зловмиснику простіше дізнатися топологію мережі, ніж з використанням радіолокаційних методів. 2) Захист конкретних даних програми залежить від вимог щодо безпеки конкретної системи.

Для подальшого розгляду оберемо SensorWare – архітектуру мережі, засновану на дослідженнях в UCLA та Науковому центрі Роквелла [1]. Звернемо увагу на аспекти архітектури, яка впливає на дизайн охорони схеми. При цьому, найважливішими елементами архітектури є: локалізовані алгоритми, локальний зв'язок та мобільний код.

Найбільш відмінною особливістю сенсорних мереж є обмежена енергія, доступна для вузлів датчиків. Отже, ретельне витрачання наявної енергії стає основним принципом проектування. Маючи на увазі, що зв'язок між вузлами споживає значну кількість енергетичних ресурсів, програмне забезпечення має досягти необхідного рівня продуктивності при мінімізації обсягу трафіку в мережі. В архітектурі SensorWare додатки розроблені на основі локалізованих алгоритмів, де вузли обмінюються повідомленнями в межах безпосереднього сусідства. Лише один центральний вузол агрегує всі показання датчиків і надсилає об’єднані дані до вузла шлюзу, який є одним із вузлів мережі і здатен служити проксі між мережею та користувачем. Будь-який вузол у мережі може бути відправником або одержувачем повідомлень. Ці властивості сенсорних мереж мають значний вплив на безпеку. У схемі безпеки, яка розглядається, ми використовуємо спільні симетричні ключі для шифрування. Таке рішення спрощує управління ключами і зберігає енергоефективність місцевого мовлення.

Парадигма мобільності коду є важливою для сенсорної мережі з двох причин: 1). Обмежена пам’ять вузлів не дозволяє постійно зберігаючи увесь додаток на вузлі. 2). Програми, які повинна запускати мережа, можуть бути невідомі на момент розгортання мережі. Оскільки ручна реконфігурація вузлів датчиків після розгортання неможлива, підтримка мобільного коду є також важливою.

Загрози безпеці у сенсорних мережах

Безпроводові мережі, як правило, більш вразливі до кібератак, ніж проводові мережі, через характер середовища передачі інформації. Крім того, безпроводові сенсорні мережі мають додаткову вразливість, оскільки вузли часто розміщуються у агресивному або небезпечному навколишньому середовищі, де вони фізично не захищені. Оскільки безпека мобільного коду сильно впливає на безпеку мережі, то захист повідомлень, що містять мобільний код, також є важливою частиною схеми безпеки зв'язку. Для типів даних, які розглядаються, можна перерахувати можливі загрози для мережі при порушенні безпеки зв'язку:

1. Вставка шкідливого коду є найнебезпечнішою атакою, яка може статися. Шкідливий код, що вводиться в мережу, може поширюватися на всі вузли, потенційно руйнуючи всю мережу, або навіть гірше, захоплюючи мережу від імені зловмисника. Вилучена сенсорна мережа може або надсилати помилкові спостереження за навколишнім середовищем законному користувачеві, або надсилати спостереження щодо відстежуваної області зловмисному користувачеві.

2. Перехоплення повідомлень, що містять фізичне розташування вузлів датчиків, дозволяє зловмисникові знаходити вузли та знищувати їх. Важливість приховування інформації про місцезнаходження від зловмисника полягає в тому, що вузли датчика мають невеликі розміри, і їх розташування неможливо простежити візуально. Таким чином, важливо приховати розташування вузлів. У разі статичних вузлів інформація про

місцезнаходження не старіє і повинна бути захищена протягом усього терміну служби мережі.

3. Окрім розташування вузлів датчиків, зловмисник може спостерігати вміст повідомлень, що стосується додатків, включаючи ідентифікатори повідомлень, позначки часу та інші поля. Конфіденційність цих полів у нашому прикладі програми є менш важливою, ніж конфіденційність інформації про місцезнаходження, оскільки конкретні дані програми не містять конфіденційної інформації і термін служби таких даних значно коротший. Також, зловмисник може вводити неправдиві повідомлення, які дають користувачеві неправильну інформацію про навколишнє середовище. Такі повідомлення також споживають певну кількість енергетичних ресурсів вузлів. Цей тип нападу називається катуванням через недосипання [6].

Схема багаторівневої архітектури захисту

Після того, як ми визначили три типи даних у мережі SensorWare та можливі загрози для мережі, можна визначити елементи схеми безпеки. Три описані тут рівні безпеки базуються на криптографії приватного ключа з використанням групових ключів. Програми та системне програмне забезпечення отримують доступ до API захисту як частини проміжного програмного забезпечення, визначеного архітектурою SensorWare. Оскільки всі три типи даних містять конфіденційну інформацію, вміст усіх повідомлень у мережі зашифрований. Ми припускаємо, що всі вузли датчиків у мережі мають доступ до вмісту будь-якого повідомлення. Як вже зазначалося раніше, ми маємо справу лише з безпекою зв'язку не обговорюючи захист самих вузлів.

Розгортання механізмів безпеки в сенсорній мережі створює додаткові накладні витрати. Затримка не тільки збільшується за рахунок виконання процедур, пов’язаних із безпекою, але й споживана енергія безпосередньо зменшує термін служби мережі. Щоб мінімізувати витрати, пов’язані з безпекою, ми пропонуємо, щоб накладні витрати на безпеку, а отже, і споживання енергії, відповідали чутливості зашифрованої інформації.

Дотримуючись таксономії типів даних у мережі, ми визначаємо три рівні безпеки:

1. Рівень безпеки I зарезервований для мобільного коду, найбільш конфіденційної інформації, що надсилається через мережу,

2. Рівень безпеки II присвячений інформації про місцезнаходження, що передається в повідомленнях ,

3. Механізм рівня захисту III застосовується до інформації про конкретну програму.

Сила шифрування для кожного з рівнів безпеки відповідає чутливості зашифрованої інформації. Отже, шифрування, яке застосовується на рівні I, є сильнішим, ніж шифрування, застосоване на рівні II, тоді як шифрування на рівні II є сильнішим, ніж кодування, що застосовується на рівні III.

Різні рівні безпеки реалізуються або за допомогою різних алгоритмів, або за допомогою одного і того ж алгоритму з регульованими параметрами, що змінюють його силу та відповідні обчислювальні накладні витрати. Використання одного алгоритму з регульованими параметрами має перевагу в тому, що займає менше місця в пам'яті. Для реалізації криптозахисту сенсорних мереж найбільш доцільним є використання RC6. RC6 підходить для модифікації рівня безпеки, оскільки він має регульований параметр (кількість раундів), який безпосередньо впливає на його міцність. Витрати для алгоритму шифрування RC6 зростають із збільшенням сили шифрування, виміряної кількістю раундів [7].

Модель багатоадресного зв'язку, властива архітектурі SensorWare, передбачає розгортання групових ключів. В іншому випадку, якщо кожна пара вузлів потребує ключа або пари ключів, зв'язок між вузлами повинен бути на основі одноадресної передачі. Це значно збільшило б кількість повідомлень. Оскільки розглядається мережа, де вузли не відстежують своїх сусідів, то один із ключів зі списку головних ключів активний у будь-який момент. Алгоритм вибору конкретного ключа ґрунтується на псевдовипадковому генераторі, що працює на кожному вузлі з однаковим ядром. Періодично та синхронно на кожному вузлі генерується нове випадкове число, яке використовується і надає та індексує запис у таблиці

доступних головних ключів. Цей запис містить активний головний ключ. Потім ключі для трьох рівнів безпеки, що відповідають трьом типам даних, отримуються з активного головного ключа. Основне припущення для усіх запропонованих схем захисту полягає в тому, що вузли датчиків ідеально синхронізовані за часом і мають точні знання про своє розташування.

Рівень безпеки I. Повідомлення, що містять мобільний код, рідше, ніж повідомлення, які екземпляри програми обмінюються на різних вузлах. Це дозволяє нам використовувати надійне шифрування, незважаючи на накладні витрати. Для інформації, захищеної на цьому рівні безпеки, вузли використовують поточний головний ключ. Набір головних ключів, відповідний генератор псевдовипадкових чисел та ядро - це дані, які потенційний користувач повинен мати для доступу до мережі. Отримавши ці дані, користувач може вставити будь-який код у мережу. Якщо зловмисний користувач порушить шифрування на цьому рівні за допомогою атаки «грубої сили», він може вставити шкідливий код в мережу.

Рівень безпеки II. Для даних, що містять розташування вузлів датчиків, пропонується інший механізм безпеки, який ізолює частини мережі, так що порушення безпеки в одній частині мережі не впливає на решту мережі. Згідно з припущеннями щодо програм, які застосовуються для роботи в сенсорних мережах, розташування вузлів датчиків, швидше за все, буде включено до більшості повідомлень. Таким чином, накладні витрати, що відповідають шифруванню інформації про місцезнаходження, суттєво впливають на загальні накладні витрати на безпеку в мережі. Це потрібно враховувати, коли визначається сила шифрування на цьому рівні. Оскільки рівень захисту для інформації про місцезнаходження нижчий, ніж для мобільного коду, ймовірність того, що ключ для рівня II може бути зламаний, вища. Маючи ключ, зловмисник може потенційно знайти всі вузли в мережі.

Щоб обмежити пошкодження лише однієї частини мережі, ми пропонуємо такий механізм безпеки. Вузли датчиків використовують ключі на основі розташування для шифрування рівня II. У разі компрометації, ключі, що залежать від розташування, можна розділити між регіонами, де розташування вузлів порушено, і областями, де вузли продовжують безпечно працювати.

Територія, покрита сенсорною мережею, розділена на комірки. Вузли в одній комірці мають спільний ключ на основі розташування, який є функцією фіксованого розташування в комірці та поточного головного ключа. Між комірками є прикордонна область, ширина якої дорівнює діапазону передачі. Вузли, що належать до цих областей, мають ключі для всіх сусідніх комірок. Це гарантує, що два вузли в межах діапазону передачі один від одного мають спільний ключ. Розміри комірок повинні бути достатньо великими, щоб локалізований характер алгоритмів у мережі забезпечував відносно низький трафік серед комірок порівняно із загальним трафіком. Ділянки можуть мати довільну форму, з єдиною вимогою, щоб була покрита вся місцевість датчика. Розподіл області на однорідні за розміром комірки є найбільш прийнятним рішенням, оскільки це дозволяє швидкому та простому способу визначити належність до комірки. Ми ділимо мережу на шестикутні комірки, оскільки це гарантує, що вузли шлюзу мають не більше трьох ключів. Частиною механізму завантаження для вузлів датчиків є процес визначення їх належності до комірки. У цьому процесі ми використовуємо поняття розширеної клітини. Розширена комірка – це гексагональна комірка, яка має той самий центр, що і вихідна комірка, а відстань між її сторонами та сторонами вихідної комірки дорівнює діапазону передачі вузлів датчика.

Рис. 2 показує три сусідні клітини та відповідні їм розширені комірки. Кожен вузол порівнює своє розташування з кожною розширеною коміркою та визначає, знаходиться він у розширеній комірці чи ні. Якщо вузол знаходиться в розширеній комірці Cx, він матиме ключ Cx, K_{Cx}. Вузли в межах прикордонних областей (затінених областей) мають кілька ключів, як показано. Наприклад, вузли, які прилягають до комірок C_1 та C_2, мають два ключі: K_{C1} та K_{C2} відповідно.

Рівень безпеки III. Ми шифруємо конкретні дані програми, використовуючи слабше шифрування, ніж те, що використовується для двох вищезазначених типів даних. Більш

слабке шифрування вимагає менших обчислювальних накладних витрат для даних, специфічних для програми. Крім того, висока частота повідомлень із даними, специфічними для програми, запобігає використанню більш сильного та ресурсоємного шифрування. Тому ми застосовуємо алгоритм шифрування, який вимагає менше обчислювальних ресурсів із відповідним зниженням рівня безпеки. Ключ, який використовується для шифрування інформації рівня III, походить від поточного головного ключа. Хеш-функція MD5 приймає головний ключ і генерує ключ для рівня III. Оскільки головний ключ періодично змінюється, відповідний протокол на цьому рівні слідкує за цими змінами.

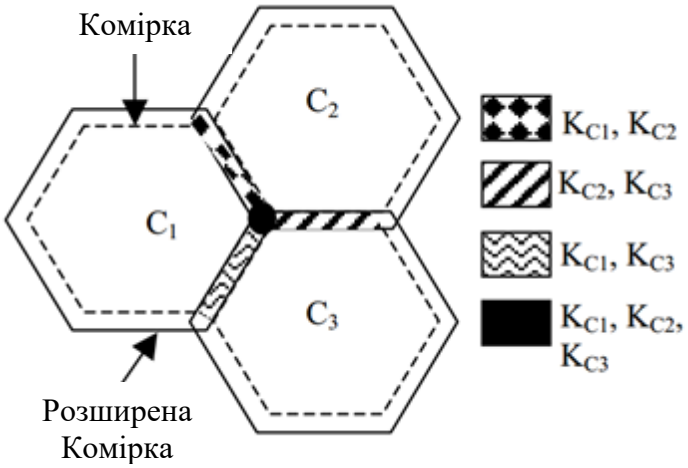

Рис. 2. Загальна структура багаторівневої архітектури захисту

Висновок

У статті запропоновано схему захисту зв'язку для сенсорних мереж на основі багаторівневої архітектури захисту. Основним результатом цієї роботи є висновок про те, що окремі механізми захисту даних з різним рівнем чутливості дозволяють ефективно керувати ресурсами, що є важливим для безпроводових сенсорних мереж. Схема, заснована на розташуванні, може захищати решту мережі, навіть коли частини мережі скомпрометовані.

Перелік посилань

1. S. Slijepcevic, M. Potkonjak, V. Tsiatsis, S. Zimbeck and M. B. Srivastava, "On communication security in wireless ad-hoc sensor networks," Proceedings. Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, Pittsburgh, PA, USA, 2002, pp. 139-144, doi: 10.1109/ENABL.2002.1030000.
2. Мулярчик Константин Сергеевич. Защита каналов коммуникации в беспроводных сенсорных сетях и системах телеметрии. Белорусский государственный университет. 2016. http://comsec.spb.ru/imctcpa16/02.03.MulyarchikKS.pdf
3. Квашенко Л.О., Кононова І.В. Аналіз методів збереження енергії в бездротових сенсорних мережах. Енергоефективні технології. 2019.
4. D. Estrin, R. Govindan and J. Heidemann, "Embedding the Internet: Introduction", Communications of the ACM, vol. 43, no. 5, pp. 38-41, May 2000.
5. Perrig, R. Szewczyk, V. Wen, D. Culler and J. D. Tygar, "SPINS: Security Protocols for Sensor Networks", MOBICOM 2001, June 2001.
6. Heshem A. El Zouka. Providing End-to-End Secure Communicationsin GSM Networks. International Journal of Network Security & Its Applications (IJNSA) Vol.7, No.4, July 2015. 31-41.
7. Philips RC-6 протокол передачи данных по ИК каналу. https://led-displays.ru/ir/philips_rc6.html

Надійшла: 09.07.2020 Рецензент: д.т.н., професор Гайдур Г.І.