УДК 621.396

ЗАХИЩЕНА БЕЗПРОВОДОВА МЕРЕЖА ДЛЯ МОНІТОРИНГУ ПАРАМЕТРІВ НАВКОЛИШНЬОГО СЕРЕДОВИЩА З МОБІЛЬНИМИ СЕНСОРАМИ

Прищепа Т.О., Валуйський С.В., Дакаєв О.В.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: sandak94@gmail.com

Secured wireless network for environmental parameters monitoring with mobile sensors

One of the main problems in the organization of wireless networks is security. To solve this problem, we suggest using a VPN connection. This ensures not only a very high level of security, but is also a convenient tool for connecting network elements.

В наш час, з кожного роком продуктивність CPU збільшується в кілька разів. Завдяки цьому, існує велика кількість невеликих мікроконтролерів, що мають високу продуктивність (наприклад, Raspberry Pi Zero, Arduino Nano). Це дає унікальну можливість для розподілу обчислювальної потужності між вузлами. Крім того, можна зробити окремий інтелектуальний вузол з широкою функціональністю, власною операційною системою і додатками, що дозволяють будувати великомасштабну розподілену безпроводову мережу датчиків для моніторингу навколишнього середовища. Але як і раніше залишається проблема безпеки і мультисервісної функціональності в таких мережах [1].

У статті запропонована модель, яка використовує концепцію Інтернету речей (Internet of Things, IoT) і являє собою зразок розподіленої безпроводової мережі для екологічного моніторингу міської місцевості (CO, забруднення повітря, вогню, шуму, рівня електромагнітного випромінювання, тощо). Дані, зібрані з фіксованих, а також мобільних датчиків моніторингу (розміщених на автомобілях, автобусах, безпілотних літальних апаратах, тощо) передаються через мережі 3G, Wi-Fi або ZigBee на віддалений сервер для подальшої обробки і візуалізації в режимі реального часу за допомогою веб-додатку. Всі канали використовують VPN з'єднання, що дозволяє створити розподілену і надійно захищену мережу.

Однією з головних проблем в організації безпроводових мереж є безпека. Щоб вирішити цю проблему, ми пропонуємо використовувати VPN з'єднання. Це гарантує не тільки дуже високий рівень безпеки, але є також зручним інструментом для з'єднання елементів мережі. Проста схема захищеної розподіленої мережі показана на рис.1.

Є чотири основних елементи, які в комплексі створюють високоефективну розподілену безпроводову сенсорну мережу. Розглянемо кожен з них.

1. Вузли. Кожен вузол складається з материнської плати, набору датчиків, безпроводового інтерфейсу і джерела живлення. Ми пропонуємо використовувати мікроконтролери як материнські плати, тому що вони досить продуктивні, щоб

використовувати VPN та для запуску деяких програм. Також, вони включають в себе деякі датчики для моніторингу параметрів навколишнього середовища міської зони, таких як CO, забруднення повітря, вогню, шуму, рівню електромагнітного випромінювання. Для безпроводового інтерфейсу, можна використовувати будь-яку доступну мережу (наприклад, GSM, Wi-Fi або ZigBee). У запропонованій моделі, вузли можуть мати власні автономні джерела живлення.

2. Мережевий інтерфейс. Що стосується нашої мережі вони можуть бути різними. Особливо, якщо ми не будемо використовувати власне джерело живлення для вузлів, ми можемо використовувати Wi-Fi, UMTS та інші потужні безпроводові мережі, не думаючи про батареї. Використовуючи нову концепцію «ZigBee-over-IP» можливо доволі просто застосувати VPN у ZigBee мережах.

3. VPN з'єднання. Для того, щоб з'єднати наші вузли і гарантувати високий рівень безпеки, пропонується використовувати VPN з'єднання. Кожен вузол використовує безпроводовий інтерфейс для підключення до сервера VPN. Після встановлення з'єднання, всі дані від вузла до сервера шифруються і передаються по VPN тунелю, інкапсулюються в спеціальних пакетах. Це дуже простий і потужний метод для побудови незалежної розподіленої мережі, тому що після усіх операцій, ми отримуємо чисту мережу, аналогічну локальній мережі з її характеристиками і функціональністю. Ми можемо не тільки отримувати дані від датчиків, але також потокове відео і аудіо дані через цю мережу. Наш VPN сервер використовує протокол GRE через порт UDP для кожного клієнта (вузла) для маршрутизації даних між мережевими елементами.

4. Сервер. Це головна і найпотужніша частина нашої мережі. Ми використовуємо декілька додатків. Перш за все, це сервер VPN, який необхідний для з'єднання наших розподілених вузлів. Другим важливим елементом є сервер бази даних - ми повинні використовувати базу даних високої продуктивності, тому що мережа доволі велика та має величезні потоки даних. Для гарної сумісності, пропонується використовувати веб-додатки, тому HTTP/HTTPS сервер необхідний для нашої системи. Для динамічної генерації веб-сторінок, також потрібний високопродуктивний сервер. Ми можемо використовувати будь-яку популярну серверну мову (наприклад, PHP або Ruby,) для наших динамічних веб-сторінок.

Тепер для розуміння принципу взаємодії розглянемо спрощену структуру мережі, яка показана на рис.2. Всі IP-адреси вузлів в цій схемі є випадковими. Ми маємо просту мережу, аналогічну звичайній локальній мережі. Використання гнучких серверних додатків VPN, дасть змогу розділити нашу мережу на певні частини і встановити маршрутизацію між ними. Наприклад, ми можемо використовувати окрему підмережу для збору даних від датчиків CO, а інша підмережа складатиметься з електромагнітних датчиків або камер і т.п. Однією з переваг VPN є те, що ми робимо нашу мережу розподіленою. Це означає, що ми зможемо використовувати наші вузли в будь-якому місці, якщо там є безпроводовий зв'язок. Наприклад, ми можемо розташувати деякі вузли в Києві, в

той час як інші будуть у Львові чи Харкові. Вони розділені географічно, але логічно – це одна мережа.

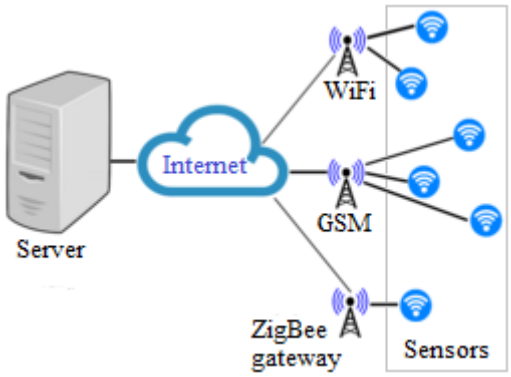

Рис. 1. Приклад архітектури мережі

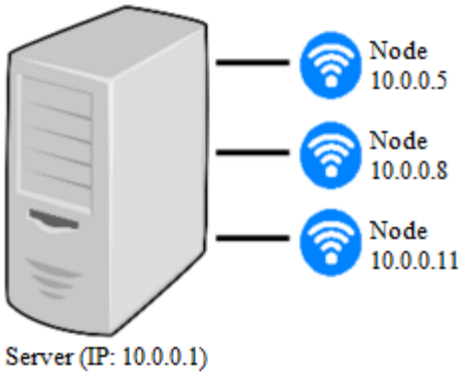

Рис. 2. Спрощена структура мережі

Використання простої мережі є дуже вигідним рішенням для нашої системи. Ми можемо дуже просто використовувати звичайні мережеві додатки, такі як веб-сервер, SSH сервер, потоковий сервер і т.д. Для потокового відео з камери, ми повинні використовувати будь-який потоковий сервер, а потім ми можемо спостерігати відео з простої адреси (наприклад, https://10.0.0.5:8000/stream) з використанням популярних відеовідтворювачів. Для даних планується використовувати відкритий API. Ми можемо використовувати формат JSON для передачі даних. Це дуже популярний формат даних, який простий у використанні з веб-додатків, баз даних та інших програм.

Висновок. Для вирішення проблеми безпеки пропонується модель захищеної безпроводової мережі за допомогою VPN-з'єднання. Також пропонується енергоефективне і компактне рішенням для побудови безпроводового вузла з датчиками, що створений на модулі XBee. Пропонується технологія для розміщення безпеки таких вузлів з використанням повітряного запуску з квадрокоптера. Датчики для моніторингу міського району можуть бути більш складним з використанням зовнішніх процесорів, а також модулів Wi-Fi або 3G. Цілі для розміщення датчиків можуть бути визначені одним з ефективних методів синтезу топології безпроводових сенсорних мереж [2].

Література

1. P. Likhar, R. S. Yadav, and K. Rao M, “Securing IEEE 802.11G WLAN Using OpenVPN and Its Impact Analysis,” International Journal of Network Security & Its Applications (IJNSA), 2011, vol. 3, №6, pp. 97-113.
2. S. Valuiskyi, O. Lysenko, T. Pryshchepa, and S. Chumachenko “The problem of finding a rational topology of wireless sensor networks using UAVs,” 2nd Int. IEEE Conf. PIC S&T, Ukraine, Kharkiv, 13-15 Oct., 2015, vol. 1, pp. 213-215.