УДК 621.396.946

ЗАХИЩЕНІ БЕЗПРОВОДОВІ МОБІЛЬНІ СЕНСОРНІ МЕРЕЖІ ДЛЯ МОНІТОРИНГУ ПАРАМЕТРІВ НАВКОЛИШНЬОГО СЕРЕДОВИЩА

Давидюк В.О., Дакаєв О.В., Димид М.Д.
Інститут телекомунікаційних систем НТУУ «КПІ»
E-mail: va.davidyuk@gmail.com, sandak94@gmail.com, mariana.dymyd@gmail.com

Secured Wireless Network with Mobile Sensors for Environmental Monitoring

In this paper technical solutions are proposed for creating secured wireless networks and sensors for environmental monitoring of urban area as well as remote contaminated area.

У наш час з кожним роком швидкодія обчислювальної техніки зростає у кілька разів. Саме завдяки цьому з'являється велика кількість досить малих, але високопродуктивних мікроконтролерів (наприклад Raspberry Pi Zero, Arduino Nano тощо). Ці пристрої надають унікальну можливість щодо розподілення обчислювальної потужності між вузлами мережі. Крім цього, можливо створювати значний функціонал для окремих вузлів зі своєю операційною системою та застосунками, що дозволяє розбудовувати широкомасштабні розподілені безпроводові сенсорні мережі для моніторингу середовища [1]. Але при цьому залишається відкритим питання безпеки та мультисервісності у таких мережах.

У даній статті запропоновано модель, яка використовує ідею інтернету речей та представляє собою зразок розподіленої сенсорної мережі для моніторингу міської зони (CO2, забруднення повітря, пожежі, шум, рівень електромагнітного поля та ін.). Дані моніторингу збираються з вузлів, що можуть розташовуватись на автомобілях, автобусах, дронах тощо, та передаються через безпроводові мережі (GSM, 3G, Wi-Fi чи ZigBee) на віддалений сервер для подальшого опрацювання та візуалізації в режимі реального часу у web-додатку. Усі канали використовують VPN-з'єднання, що забезпечує розподіленість та безпеку мережі [2].

Одною з найбільших проблем безпроводових сенсорних мереж є безпека даних. Для вирішення даного питання ми пропонуємо використання VPN. Це рішення гарантує не тільки високий рівень безпеки, а також надає чудовий метод з'єднання елементів мережі. Зразок такої розподіленої мережі показано на рис. 1.

Існує 4 основні елементи, які в сумі дають високопродуктивну розподілену безпроводову сенсорну мережу.

1. Вузли. Кожен вузол містить материнську плату, сенсори, безпроводовий інтерфейс та джерело живлення. Ми пропонуємо використання мікроконтролерів у якості материнських плат, адже вони достатньо продуктивні для використання VPN та запуску додатків [2]. Для моніторингу середовища існують сенсори що моніторять параметри (CO, забруднення

повітря, пожежі, шум, рівень електромагнітного поля та ін.). В якості безпроводового інтерфейсу використаємо будь-яку доступну мережу (GSM, Wi-Fi або ZigBee). У запропонованій моделі вузли матимуть власні автономні джерела живлення.

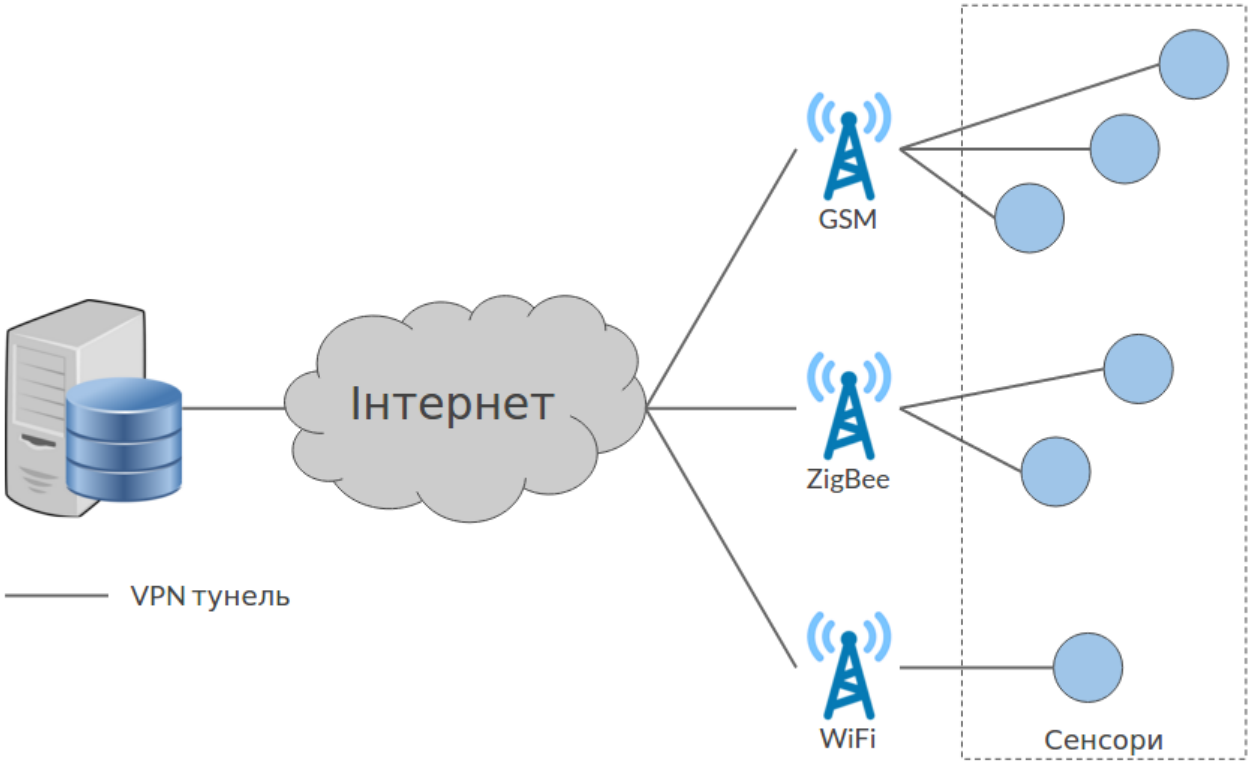

Рис. 1. Архітектура системи.

2. Мережевий інтерфейс. У нашому випадку, є досить великий вибір технологій. Якщо не буде використовуватись автономне джерело живлення, можливе застосування WiFi, UMTS та інших енергозатратних безпроводових рішень. Використання нової концепції 'ZigBee-over-IP' досить сильно спрощує використання VPN у мережах ZigBee.

3. VPN-з'єднання. Для того, щоб з'єднати вузли в мережу та гарантувати високий рівень безпеки даних, пропонується використовувати VPN. Кожен вузол використовує свій радіоінтерфейс для підключення до VPN-сервера. Після встановлення з'єднання, усі дані від вузла до сервера шифруються та передаються через VPN-тунель, перед цим енкапсульовані у спеціальні пакети. Даний метод є дуже простим та ефективним для побудови незалежної розподіленої мережі, адже після усіх виконаних дій ми отримуємо повноцінну мережу, подібну до локальної по характеристикам та функціоналу. Більше того, крім передачі даних з сенсорів через мережу є можливість транслювати потокове аудіо або відео. Наш VPN-сервер використовує протокол GRE через UDP-порт для кожного клієнта (вузла) для маршрутизації даних між елементами мережі.

4. Сервер. Саме він є найважливішим елементом мережі. Ми використовуємо кілька додатків на сервері. Перший – VPN-сервер, який необхідний для з'єднання розподілених вузлів. Другий важливий додаток –

сервер баз даних – необхідно використовувати високопродуктивну базу даних для великомасштабної мережі та великих потоків даних. Для хорошої сумісності рекомендується використовувати веб-додатки, отже стає необхідною наявність HTTP/HTTPS-серверу для нашої системи. Для динамічної генерації веб-сторінок можливо застосувати будь-яку поширену мову програмування, наприклад PHP або Ruby.

Однією з сучасних тенденцій у телекомунікаційних системах є використання безпілотних літаючих апаратів (БПЛА), які підтримуються нашей мережею [3]. Є можливість приєднати вузол до БПЛА та збирати дані у різних географічних зонах. За допомогою сенсора GPS відкривається можливість додавати геотеги до зібраних даних, за допомогою яких створювати потужні системи моніторингу з застосуванням інтерактивних карт. Наприклад, після пожежі на певному об'єкті доцільно використовувати БПЛА з сенсорами забруднення повітря, після чого створити інтерактивну карту, на якій можна буде побачити актуальні рівні забруднення по території, отже населення зможе вжити певних заходів, наприклад покинути територію або закрити вікна.

Таким чином, для розв'язання проблеми з безпекою доцільно застосовувати VPN – з'єднання. Крім цього, для енергоефективного і компактного рішення пропонується побудова мережі на основі модулів XBee. Для безпечного розміщення вузлів у зонах аварій чи лиха можливе використання БПЛА [3]. У міській зоні є змога використовувати більш складні сенсори з використанням зовнішніх процесорів, а також модулів Wi-Fi або 3G.

У даній статті розглянута досить проста, проте потужна ідея побудови розподіленої безпроводової мобільної сенсорної мережі для моніторингу параметрів навколишнього середовища. Запропонована система має значні переваги у безпеці даних, простоті побудови та простоті управління. В подальшому, система матиме значний потенціал щодо модернізації та впровадження новітніх розробок, зокрема, нових систем автоматизації різноманітних процесів та нових систем моніторингу, обліку та візуалізації даних. Ці питання будуть надалі розв'язуватись та розглядатимуться у подальших публікаціях.

Література

1. Лисенко О.І., Нікулін О.Ф., Чумаченко С.М., Валуйський С.В. Задача оптимального розміщення сенсорів. Технології екологічного моніторингу із використанням інтелектуальної сенсорної техніки // Проблеми телекомунікацій: 8-а Міжнар. наук.-техн. конф., 22-25 квіт. 2014р. : матеріали конф. – К., 2014. – С. 53-56.
2. 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.
3. 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.