

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДВНЗ «УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ СИСТЕМ

«ТЕХНОЛОГІЇ РОЗУМНОГО МІСТА»
(SMART CITY TECHNOLOGIES)

Методичні вказівки до лабораторних робіт

УЖГОРОД - 2024

Технології розумного міста» (Smart city technologies): методичні вказівки до лабораторних робіт для здобувачів другого (магістерського) рівня вищої освіти, спеціальності 121 Інженерія програмного забезпечення факультету інформаційних технологій УжНУ / Укладачі: к. ф.-м. н., доц. Петрушко І.А., Поліщук І.В., к. ф.-м. н., доц. Білак Ю.Ю. – Ужгород: 2024. – 43 с.

У методичних вказівках з курсу «Технології розумного міста» (Smart city technologies) розглянуто перелік тем, що входять до складу робочої програми. До лабораторних робіт сформульовано короткі теоретичні відомості, вказано завдання та хід виконання, а також критерії правильності виконання поставлених завдань. У методичних вказівках наведено перелік запитань для підсумкового контролю знань та список рекомендованої літератури.

Укладачі:

Петрушко І.А., к. ф.-м. н., доц., доцент кафедри програмного забезпечення систем ДВНЗ «УжНУ»;

Поліщук І.В., асистент кафедри програмного забезпечення систем ДВНЗ «УжНУ»;

Білак Ю. Ю., к. ф.-м. н., доц. завідувач кафедри програмного забезпечення систем ДВНЗ «УжНУ».

Рецензенти:

Повхан І.Ф., д.т.н., проф., декан факультету інформаційних технологій ДВНЗ «УжНУ»;

Маслюк В. Т., д.ф.-м.н., проф., завідувач відділом фотоядерних процесів ІЕФ НАНУ.

Рекомендовано кафедрою програмного забезпечення систем від «15» травня 2024р., протокол №11.

Розглянуто і схвалено науково-методичною комісією факультету інформаційних технологій УжНУ. Протокол №7 від 17.05.2024 р.

Зміст

Вступ	4
Лабораторна робота № 1.	
Розумне паркування та управління транспортними потоками.....	5
Лабораторна робота № 2.	
Розумна енергетична мережа.....	12
Лабораторна робота № 3.	
Інтернет речей в медицині: допомога пацієнтам з цукровим діабетом.....	16
Лабораторна робота № 4.	
Розумна будівля.....	23
Лабораторна робота № 5.	
Захист хмарних сервісів інтернету речей в розумній будівлі.....	29
Лабораторна робота № 6.	
Еволюція безпекових опцій в протоколах WiFi зв'язку.....	34
Рекомендовані джерела інформації	42

Вступ

З ростом популярності Інтернету речей (IoT) зростає потреба у фахівцях, які володіють навичками програмування та налаштування різноманітних пристроїв IoT. У сучасному світі використання інтелектуальних систем стає стандартом як у повсякденному житті, так і на промисловому рівні. Щоб успішно впроваджувати інтелектуальні пристрої, потрібно розробляти спеціалізоване програмне забезпечення для налаштування їхньої роботи в мережі та забезпечувати їхню безпеку від несанкціонованого доступу.

Метою вивчення дисципліни «Технології розумного міста» є формування навичок розробки програмного забезпечення для централізованого адміністрування мереж IoT відповідно до визначених вимог. Студенти також здобувають вміння програмно-налаштовувати пристрої IoT для їх ефективної роботи в мережі з використанням визначеної топології.

Мета лабораторного практикуму полягає в набутті практичних навичок програмування та налаштування пристроїв мереж IoT. В ході практикуму студентам надаються теоретичні матеріали, завдання на лабораторні роботи, методичні вказівки для їх виконання, вимоги до звітів та рекомендована література. Всі лабораторні роботи виконуються в середовищі Cisco Packet Tracer на платформі Cisco Networking Academy, в межах курсу IoT Connecting Things.

Навчальний посібник призначений для студентів, які навчаються за спеціальністю 121 «Інженерія програмного забезпечення» факультету інформаційних технологій ДВНЗ «Ужгородського національного університету».

Лабораторна робота № 1

РОЗУМНЕ ПАРКУВАННЯ ТА УПРАВЛІННЯ ТРАНСПОРТНИМИ ПОТОКАМИ

Мета роботи: ознайомитися з принципами організації інтернету речей (IoT) розумного міста, а також дослідити IoT рішення для системи розумного паркування та управління транспортними потоками в місті.

Обладнання: симулятор Cisco Packet Tracer (PT).

Теоретичні відомості

Близько тридцяти відсотків заторів у центрі міста спричинюються водіями, які шукають місце для паркування, та ще двадцять п'ять відсотків - завдяки дорожньо-транспортним пригодам. У розумних містах завдяки системі датчиків та активаторів (IoT-системі) ці проблеми можна вирішити за допомогою простих рішень. IoT від англійського Internet of Things. Загальна схема керуючої системи наступна [1, с. 28]:

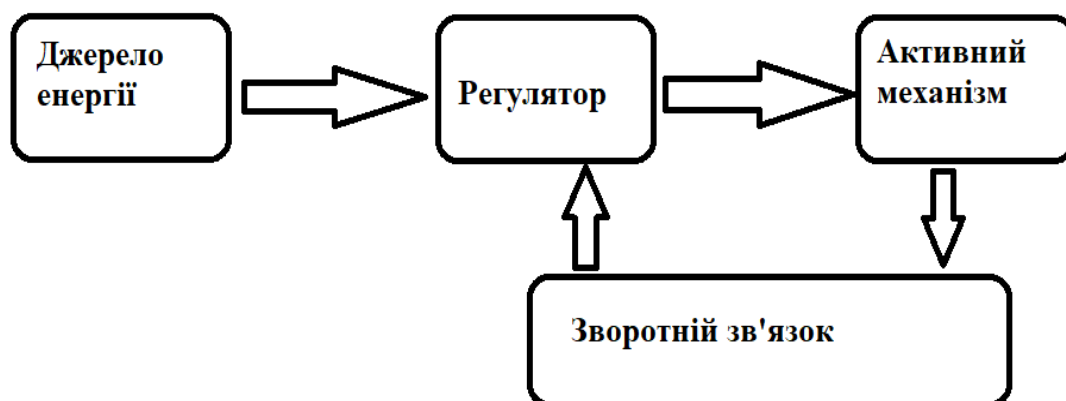


Рис. 1.1 Логічна схема IoT системи.

Джерело енергії живить систему. Регулятор керує активним механізмом IoT системи завдяки наперед написаним програмам. Алгоритми програм є мультिकанальними – в програмних сценаріях прописано залежність від зовнішніх даних. Активний механізм виконує ці програмно-зумовлені дії. Зворотній зв'язок - це система датчиків, які вимірюють деякі параметри зовнішнього середовища (температура, тиск, провідність і т.д.), передає ці дані

в регулятор для того, щоб обрати/налаштувати програмний сценарій керування активним механізмом. Така схема є універсальною для більшості керуючих систем: від суспільних систем до живих організмів. Детальний опис IoT систем подано в літературі [2-7].

В даній роботі ми вивчатимемо рішення Cisco Smart + Connected Parking, яке забезпечує мешканців міста актуальною інформацією про вільні місця для паркування і дає можливість забронювати їх заздалегідь через мобільні додатки. В такий спосіб вдається покращити рух на дорогах та забезпечити співпрацю між містами, мешканцями, місцевими підприємствами та органами влади з метою ефективного контролю за паркуванням. Рішення Cisco Smart + Connected Traffic дає змогу здійснювати моніторинг міського трафіку, що дозволяє органам управління трафіком ефективно реагувати на негайні інциденти та планувати довгострокові заходи для оптимізації ситуації на дорогах.

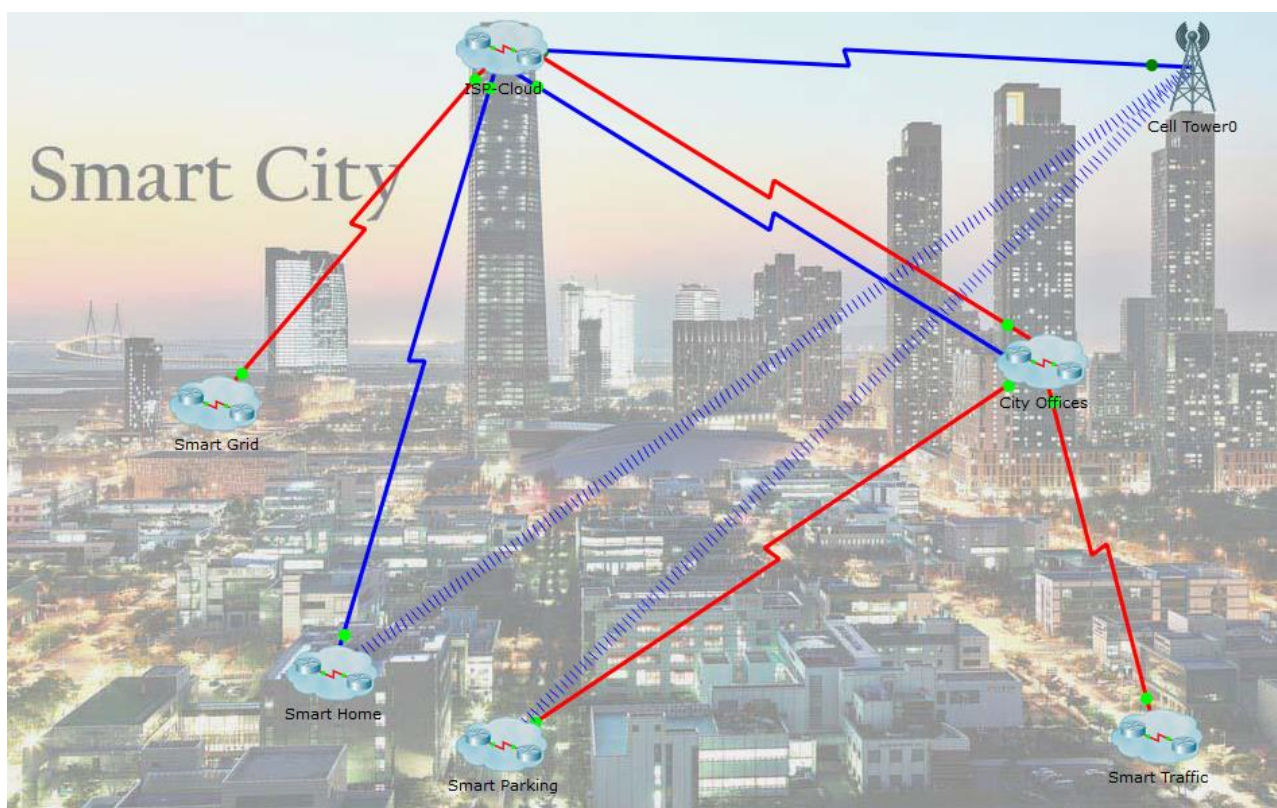


Рис. 1.2 Топологія комп'ютерної мережі IoT мережі розумного міста

Оскільки датчики та пристрої IoT розподілено по розумному місту, необхідна відповідна комунікаційна інфраструктура. Розумне місто - це столична мережа MAN (Metropolitan Area Network), що складається з менших мереж. Ці мережі часто з'єднуються в WAN (Wide Area Network - це тип мережі, яка охоплює велику географічну область; на відміну від локальної мережі LAN, яка зазвичай охоплює невелику область, наприклад, будівлю або офісний комплекс, WAN може охоплювати місто, країну або навіть весь світ.) WAN організують зв'язок на великих географічних відстанях. Хмара ISP забезпечує широкий доступ до міста для різних осіб та організацій.

Пристрої в групі розумної парковки можна контролювати віддалено з будь-якого комп'ютера в групі міських офісів. Оскільки всі пристрої групи розумної парковки підключаються до міського сервера IoT, на якому розміщений веб-інтерфейс, планшети, смартфони, ноутбуки або настільні комп'ютери можна використовувати для взаємодії зі смарт-пристроями.

Послідовність виконання роботи

1. Натисніть ISP Cluster та ознайомтеся з ресурсами, які він пропонує місту. Натисніть кнопку назад. Які міські мережі підключені за допомогою червоних послідовних кабелів?

2. Розглянемо міські офіси. Які міські мережі підключені за допомогою синіх коаксіальних кабелів?

3. Стільникова вежа, домашні та міські офіси. Натисніть на групу "Міські офіси". Чому до ISP Cloud ведуть два з'єднання?

4. Натисніть кнопку назад. Які міські мережі бездротово під'єднані до стільникової вежі?

5. Які пристрої в Smart Home під'єднані до стільникової вежі?

6. Які пристрої в групі Smart Parking під'єднані до Cell-Tower?

7. Звернемося до розумне паркування. Натисніть City IT Laptop в групі міських офісів.

Перейдіть до Desktop > Web Browser.

8. У адресному рядку введіть 195.0.0.2. Це IP-адреса сервера City IoT.

Використовуйте Park / Park як ім'я користувача та пароль для входу в City IoT Server.

Примітка: Вам може знадобитися кілька хвилин, поки всі мережеві пристрої не стануть онлайн, і лічильники парковки зможуть дістатися до сервера реєстрації IoT.

Що відображається?

9. Список усіх розумних пристроїв, які зараз підключені до сервера City IoT.

Деякими пристроями можна керувати, а інші - лише під контролем.

Лічильники паркування зареєструються на сервері та періодично надсилають оновлення статусу. Клацніть P-Space-1 метр, щоб розгорнути його.

Яке значення відображається?

10. Не закриваючи вікно City IT Laptop, поверніться до групи розумного паркування, натисніть та перетягніть червоний автомобіль на паркувальне місце 1. Місце для паркування 1 - це найлівіше місце для паркування в групі.

11. Поверніться до вікна City IT Laptop і знайдіть P-Space-1 (при необхідності розкрийте його).

Яке значення відображається тепер?

Датчики паркувальних місць - це датчики провідності (підібрані в симуляторі РТ), виконані з можливістю реагувати на металеві предмети (автомобілі в даному випадку), якщо їх розмістити досить близько.

12. Взаємодія з інтелектуальною паркувальною групою (звичайні громадяни)

Хоча це корисно як інструмент моніторингу для міської адміністрації, звичайні громадяни не повинні мати доступу до інтерфейсу на сервері. Щоб громадяни могли контролювати, які місця для паркування є на даній вулиці, була розроблена ще одна веб-сторінка.

13. Закрийте вікно City IT Laptop и поверніться до групи Smart Parking.

Натисніть на смартфон і відкрийте його веб-браузер, перейшовши на вкладку «Робочий стіл»> «Веб-браузер».

Наберіть в адресному рядку 10.10.10.10. 10.10.10.10 - адреса сервера паркування, представлена РТ-MSU.

Примітка. Завантаження сторінки в веб-браузері смартфона може зайняти кілька секунд.

Що ви бачите після завантаження сторінки?

14. Не закриваючи вікно смартфона, перетягніть зелений автомобіль на місце для паркування 5. Місце для паркування 5 - це найправіше місце для паркування в інтелектуальній парковці.

Поверніться до вікна смартфона (веб-браузер все одно повинен відображати сторінку, завантажену з сервера паркування MSU). Що ви бачите після завантаження сторінки?

Примітка: Оновлення сторінки може зайняти кілька секунд.

Місця для паркування не тільки звітують до сервера реєстрації IoT, розміщеного в групі City Offices, але й звітують перед місцевим сервером паркування. Це дозволяє громадянам переглядати та дізнаватися про наявність місця для паркування ще до того, як вони прибудуть до місця парковки.

15. Знайдіть деякий час, щоб вивчити код, який працює в MCU Parking Server

16. Звернемося до організації розумного дорожнього руху

Ще одна складова розумного міста - Smart Traffic. У цьому прикладі Smart Traffic дозволяє аварійним транспортним засобам, таким як швидка допомога або парамедики, комунікувати з системою світлофора та вимагати термінового проїзду в разі надзвичайної ситуації. Перейдіть до групи Smart Traffic.

У цьому прикладі Street Light 1 та Street Light 2 грають роль світлофорів. Парамедики реагують на надзвичайну ситуацію. Коли автомобіль парамедиків наближається до світлофорів, вони стають зеленими.

Натисніть і перетягніть вантажівку медпрацівників і помістіть її ближче до світлофора справа, який в даний час червоний.

17. Що відбувається зі світлофором праворуч?

18. Відсуньте парамедиків від світлофора праворуч і поставте його поруч із червоною машиною. Що відбувається зі світлофором?

19. Автомобіль медиків відправляє повідомлення в MCU, яке контролює світлофори, і вимагає проходу. MCU визнає транспорт медиків законним транспортним засобом та надає йому проїзд, змінивши світло на зелений. MCU також включає відповідні індикатори червоного

кольору для забезпечення безпечного проходу. Коли аварійний автомобіль пройшов безпечно, MCU повертає систему до нормальної роботи.

20. Витратьте деякий час на аналіз коду, що працює в MCU в машині швидкої допомоги, перейшовши на вкладку Програмування.

Примітка. Можливо, вам потрібно буде натиснути кнопку Додатково в нижній частині вікна пристроїв, перш ніж відобразиться вкладка «Програмування».

Поміркуйте про наступне: коли датчики, програмне забезпечення та сервери взаємопов'язані, як можна збирати дані та стежити за подіями; як приймати рішення на основі даних, керованих подіями; як пов'язані речі можуть контролювати та діяти завдяки програмам, датчикам, активним механізмам, поєднаним мережею.

Контрольні запитання

1. Дайте означення поняттю IoT системи. Яка роль зворотнього зв'язку в системі керування IoT системою ?
2. Дайте означення WiFi зв'язку, як організовано зв'язок в IoT системі розумного міста?
3. Що таке датчик? Якими датчиками обладнані розумні парковки?
4. Як організовано розумний світлофор ? Відкоментуйте скрипт, що керує роботою розумного світлофора.

Лабораторна робота № 2

РОЗУМНА ЕНЕРГЕТИЧНА МЕРЕЖА

Мета роботи: дослідити організацію інтернету речей (IoT) розумної енергетичної системи (Smart Grid), вивчити роль хмарних досліджень в розумній енергетичній системі.

Обладнання: симулятор Cisco Packet Tracer (PT).

Теоретичні відомості

У цій лабораторній роботі ми розглянемо IoT систему розумного міста та його Smart Energy Grid - розумну енергосистему [2-7]. Розумна енергосистема моніторить потужність, що подається з різних джерел, і переходить на найефективніше доступне джерело живлення. Розумна енергосистема використовує переваги інтелектуального комутатора, щоб вирішити, яке джерело живлення використовувати.

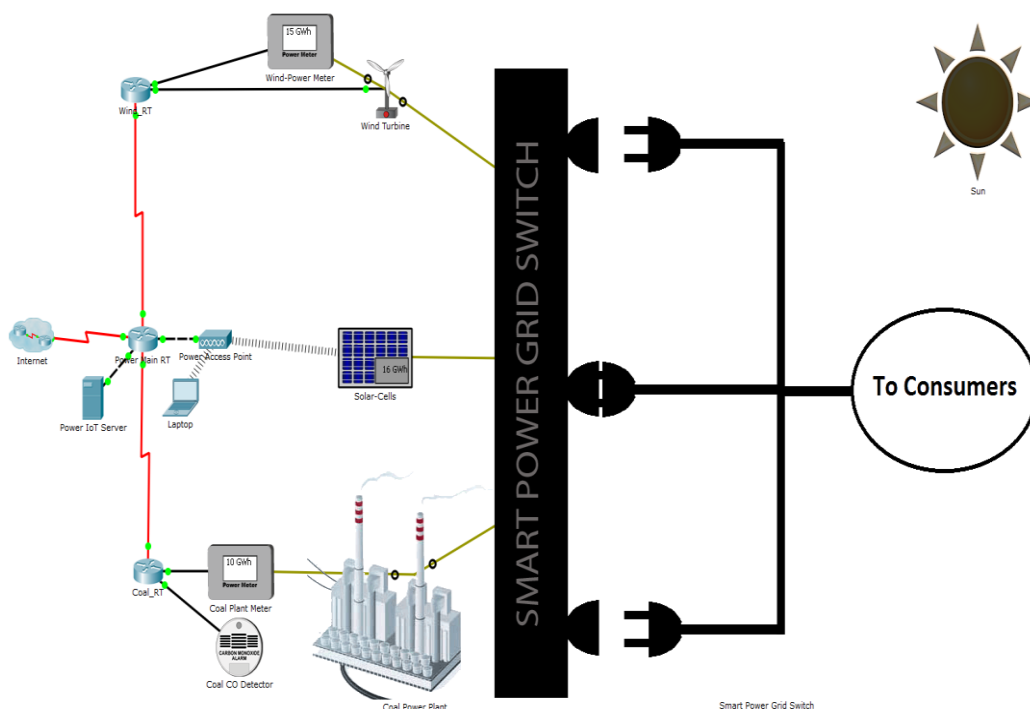


Рис. 2.1 Топологія Smart Energy Grid

Розглянемо пристрої, які є основою розумної енергосистеми. Мережеві пристрої необхідні для забезпечення зв'язку в Розумній енергосистемі. Сонячні елементи, вітрові турбіни і вугільна електростанція відповідають за

вироблення енергії. Лічильники та датчики використовуються для збору даних та полегшення моніторингу джерел енергії.

Ключовим аспектом IoT є “інтелект”, програма, яка керує роботою системи. Програми дозволяють пристроям та приймати рішення на основі подій-тригерів або зовнішніх подій (зворотній зв'язок). Перед тим, як програми можуть бути виконані речами, необхідно встановити належну апаратну платформу, по суті, перетворивши річ у комп'ютер. Зазвичай це робиться шляхом додавання процесора, пам'яті та певної можливості вводу/виводу. Нарешті, новостворена розумна річ повинна мати зв'язок з інтернетом, щоб стати частиною IoT. Саме мережеві пристрої дозволяють Smart Power Grid Switch комунікувати по мережі та утворювати єдину систему IoT.

Packet Tracer позначає з'єднання між мережевими пристроями, але їх можна відключити для зручності читання. Щоб увімкнути маркування, перейдіть до Options > Preferences > Interfaces Tab > і поставьте галочку Show Port Labels in Logical Workspace (Завжди показувати мітки портів у логічній робочій області).

Послідовність виконання роботи

Крок 1: Дослідимо хмару Розумної енергосистеми.

Натисніть на хмару Розумної енергосистеми. Скільки маршрутизаторів ви бачите в ній? Як вони називаються?

a. Яка функція маршрутизаторів?

b. У Розумній енергосистемі використовується бездротова точка доступу. Яке її ім'я? Яка його функція?

c. Чи є спосіб дізнатися, яке джерело енергії активно виробляє енергію?

d. Який пристрій відповідає за перемикання між різними джерелами живлення?

e. Як Smart Grid визначає, яке джерело живлення використовувати?

f. Що таке IP-адреса сервера Power IoT?

g. Ноутбук використовується технічними фахівцями для контролю кількості енергії? Використовуйте веб-браузер для віддаленого підключення до Power IoT-сервера. Вам потрібно знати ім'я користувача та пароль для входу на Сервер. Ви можете виявити ім'я користувача та пароль, вивчивши інші пристрої в Розумній енергосистемі. Що таке ім'я користувача та пароль та за допомогою якого пристрою ви його виявили?

Крок 2: Вивчення Smart Power Grid Switch

Smart Power Grid Switch може запускати різні сценарії програми приєднання до певного джерела живлення. Спочатку моніторимо рівні електроенергії з усіх джерел (вітроелектростанція, сонячні батареї та вугільна установка) та вирішуємо, яке джерело найкраще.

a. Натисніть **перемикач Smart Power Grid**.

b. Перейдіть на вкладку **Programming**. Якщо вкладку **Programming** не видно, натисніть кнопку **Advanced** внизу вікна, щоб відобразити розширені вкладки.

c. У лівій частині вкладки Програмування двічі натисніть **power_switch (Javascript)**, а потім двічі натисніть **main.js**. Програма Javascript, що

працює на Smart Power Grid Switch, повинна з'являтися в правій частині вкладки Programming.

Місцерозташування електромережі освітлюється з 6 год. до 18 год (з 6 ранку до 18 вечора). Через близькість до океану вітер зазвичай дме з 3 год до 22 год (з 3 ранку до 10 вечора). Програма гарантує, що сонячна енергетика є найбільш оптимальним джерелом енергії. Якщо сонячної енергії немає (немає сонячного світла), програма переходить на енергію вітру, якщо він є. Якщо не дме вітер, програма повертається до енергетики на вугіллі.

- d. Який розділ програми прояснює цю перевагу (сонячна батарея> вітрогенерація> вугільна теплоелектростанція)?
-

Контрольні запитання

1. Як організовано розумну енергосистему ?
2. Відкоментуйте роль WiFi зв'язку розумної енергосистеми ?
3. Які ще інтелектуальні приладі можна використати для вдосконалення роботи розумної енергетичної мережі?
4. Запропонуйте методи покращення рівня безпеки розумної енергетичної мережі.
5. Проаналізуйте код, що керує роботою розумної енергомережі.

Лабораторна робота № 3

ІНТЕРНЕТ РЕЧЕЙ В МЕДИЦИНІ (IoT): ДОПОМОГА ПАЦІЄНТАМ З ЦУКРОВИМ ДІАБЕТОМ

Мета роботи: ознайомитися з основними поняттями IoT технологій в сфері медицини, дослідити IoT рішення для моніторингу хворих з цукровим діабетом в симуляторі Cisco Packet Tracer.

Обладнання: симулятор Cisco Packet Tracer.

Теоретичні відомості

Інтернет речей (англ. Internet of Things, IoT) є концепцією мережі, яка є системою взаємопов'язаних механічних і цифрових пристроїв, об'єктів, тварин або людей, які мають програмне забезпечення, що дозволяє здійснювати передачу та обмін даними між фізичним світом та комп'ютерними системами за допомогою стандартних протоколів зв'язку. Така мережа може мати датчики та виконавчі механізми, вбудовані у фізичні та/або живі об'єкти і пов'язані між собою через дротові чи бездротові мережі. Ці взаємопов'язані пристрої можуть зчитувати та приводити в дію, програмуватися та ідентифікувати пристрої без участі людини за рахунок використання інтелектуальних інтерфейсів. Основною концепцією інтернет протоколу (IP) є можливість підключення різних об'єктів (речей), які людина може використовувати у повсякденному житті. Це можуть бути такі пристрої, як кавоварка, холодильник, кондиціонер, автомобіль. Такі об'єкти (речі) повинні мати вбудовані сенсори для обробки інформації, що надходить з навколишнього середовища, обмінюватися нею і виконувати різні дії в залежності від отриманої інформації. Прикладом є система «розумний будинок» або «розумна ферма». Ця система аналізує дані навколишнього середовища (температура, вологість, освітлення, ...) і, наприклад, в залежності від показників, регулює температуру в приміщенні. У зимовий період регулюються інтенсивність опалення, у спеку будинок має механізми відчинення і зачинення вікон, завдяки чому будинок провітрюється, причому

все це відбувається без втручання людини. Для об'єднання побутових речей у мережу необхідно використати декілька технологій. Система унікальної ідентифікації дозволяє збирати та накопичувати інформацію про предмети. Це можна забезпечити за допомогою мікросхем RFID (Radio-Frequency Identification). Вони здатні без власного джерела струму передавати інформацію приладам зчитування. Кожна мікросхема має індивідуальний номер. Для визначення точного місцеположення пристрою використовується технологія GPS (Global Positioning System). Для відслідковування змін у стані елементу або оточуючого середовища об'єкти оснащуються сенсорами. Для обробки та накопичення даних з сенсорів використовується вбудований комп'ютер (наприклад, Raspberry Pi, Intel Edison тощо). Для обміну інформацією між пристроями можуть бути використані технології бездротових мереж (Wi-Fi, Bluetooth, ZigBee, 6LoWPAN). Інтеграція з мережею Інтернет передбачає використання IP-адреси як унікального ідентифікатора. Об'єктами в IP будуть не тільки пристрої із сенсорними можливостями, але й пристрої, які виконують дії (наприклад, лампочки або замки, якими можна керувати через мережу Інтернет). Важливими характеристиками бездротової передачі даних для побудови IoT є ефективність, відмовостійкість, адаптивність та можливість самоорганізації. Оскільки усі пристрої під'єднані до мережі Internet, вони реєструються на сервері реєстрації, дозволяючи користувачеві контролювати всю систему з веб-браузера. Коли пристрої належним чином під'єднані, вони повинні бути налаштовані. Оскільки система покладається на інтернет мережу, пристрої повинні бути налаштовані з правильною інформацією про IP-адреси. На рис. 3.1 зображені пристрої, які можна використовувати як рішення IoT для моделювання та тестування їх роботи в середовищі Cisco Packet Tracer.

діагностували діабет 5 років тому, і йому важко підтримувати нормальний рівень глюкози. Також, мала місце госпіталізація та діабетична кома. Якщо рівень цукру виходить за межі допустимого, система моніторингу здоров'я надсилає сповіщення на пристрої Джона і він має відповісти, чи все гаразд. Якщо Джону не вдається зв'язатися з системою моніторингу здоров'я, до нього буде направлено медичний персонал (**Мобільна Медична Станція ММС**, рис. 3.2). щоб відновити нормальний рівень глюкози і запобігти діабетичну кому.

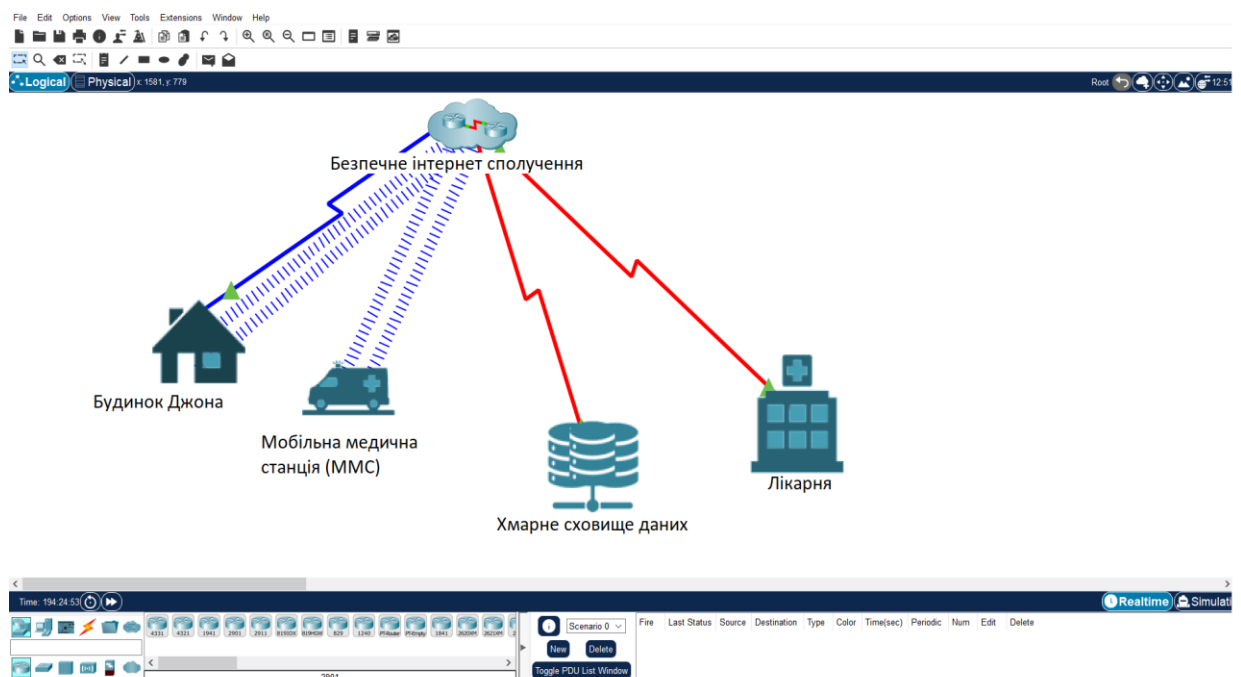


Рис. 3.2. IoT рішення для пацієнтів з цукровим діабетом у середовищі моделювання Cisco Packet Tracer

Послідовність виконання роботи

1. Налаштуйте пристрої для під'єднання.

Налаштовуємо маршрутизатор Джона на використання DHCP протоколу для призначення IP-адрес його пристроям із підтримкою IP у його домі.

1.1. Натисніть **Дім Джона**.

1.2. Натисніть маршрутизатор Home Gateway.

1.3. Натисніть вкладку GUI.

1.4. Під заголовком «Налаштування мережі» призначте IP-адресу маршрутизатора 192.168.0.1. Виберіть 255.255.255.0 для маски підмережі.

1.5. Щоб запустити сервер DHCP, клацніть «Увімкнено» поруч із «DHCP-сервером». Натисніть «Зберегти налаштування», щоб зберегти зміни.

2. Досліджуємо пристрої IoT.

2.1. Перегляньте життєві показники Джона на планшеті в **Мобільній Медичній Станції (ММС)**.

Медичний персонал у ММС може контролювати показники Джона, коли вони йдуть до Джона додому. Медичний персонал також може отримати код розблокування, щоб увійти в будинок Джона, якщо Джон не відповідатиме.

а) Відкрийте один із планшетів у ММС.

б) Натисніть вкладку HC Mobile Monitoring Web Application, щоб переглянути життєві показники Джона.

3. Провокуємо подію (гіпоглікемію або гіперглікемію), яка змусить Джона потребувати медичної допомоги.

3.1. У вкладці Environment (Condition Controller Dashboard) ви можете впливати на рівень глюкози Джона. Коли рівень глюкози Джона не буде в межах норми, **Лікарня** надішле Джону сповіщення на його під'єднані пристрої, щоб запропонувати йому зателефонувати їм, щоб вони могли оцінити його стан і надіслати медичну допомогу, якщо необхідно.

На інформаційній панелі у вікні середовища (Condition Controller Dashboard) ви можете викликати гіпоглікемію, гіперглікемію або відновити його рівень глюкози до нормального діапазону.

3.2. Імітуємо гіперглікемію: Джон не був стриманим у їжі під час сімейної вечері у себе вдома. Також, він знехтував прийомом інсуліну.

а. Перейдіть на вкладку веб-програми HC Mobile Monitoring на планшеті, щоб контролювати рівень глюкози.

- б. Перейдіть до вкладки **Wearable Watch with Sensors** на його розумному годиннику, щоб контролювати рівень глюкози.
- в. У вікні **Environment** клацніть **Induce Hyperglycemia**, щоб підвищити рівень цукру в крові, імітуючи гіперглікемію.
- г. Слідкуйте за сповіщеннями на розумному годиннику та планшеті Джона. Які дії має зробити Джон у цей час?

Скільки часу знадобиться для надсилання допомоги?

Ігноруйте попередження. Що відбувається, коли він не реагує?

- д. Відновіть життєві функції Джона до нормального рівня.

3.3. Імітуємо гіпоглікемію.

Джон пропустив обід і заснув, дивлячись телевизор. Рівень глюкози у Джона впав до небезпечного.

- а) Перейдіть на вкладку веб-програми **HC Mobile Monitoring** на його смартфоні, щоб контролювати його життєві показники.
- б) У вікні «**Environment**» клацніть «**Викликати гіпоглікемію**», щоб знизити рівень цукру в крові, імітуючи гіпоглікемічну подію.
- в) Спостерігайте за сповіщеннями на всіх його пристроях і на планшеті **Мобільної Медичної Станції (ММС)**.

Якщо Джон не вживе необхідних заходів для повернення свого рівня глюкози до нормального діапазону, він отримає сповіщення від **Лікарні**, з проханням зателефонувати їм, щоб вони могли оцінити його стан. Якщо Джон не відповість на сповіщення, **Мобільна Медична Станція (ММС)** буде направлена до нього додому для надання медичної допомоги.

Зверніть увагу на сповіщення на планшеті **ММС**.

Що відбувається, коли відправляється ММС?

Скільки часу знадобиться для прибуття ММС?

Що відбувається, коли прибуває ММС?

г) Відновіть життєві функції Джона до нормального рівня.

Контрольні запитання

1. Пояснити термін та концепцію медичних IoT систем. Які IoT пристрої було використано для моніторингу стану пацієнта?
2. Які технології використовуються для обміну інформацією між пристроями? Поясніть, будь ласка, роль IP адреси.
3. Які можливості середовища Cisco Packet Tracer для створення та налаштування IoT рішень ви знаєте?
4. Запропонуйте власне IoT рішення для моніторингу стану пацієнта і для реагування на його стан.

Лабораторна робота № 4

РОЗУМНА БУДІВЛЯ

Мета роботи: ознайомитися з принципами організації інтернету речей (IoT) розумної будівлі як частини розумного міста, а також дослідити туманні обчислення на прикладі IoT рішення для системи розумного будинку.

Обладнання: симулятор Cisco Packet Tracer.

Теоретичні відомості

У цій лабораторній роботі ми дослідите приклад розумного дому. Залежно від програми деякі дані найкраще обробляються поблизу джерела – це і є туманні обчислення. Перевагою туманних обчислень є забезпечення успішної роботи IoT системи розумного будинку навіть при відсутності Internet зв'язку (стихійні лиха, пожежі і т. д.) Приклад розумного будинку використовує туманну обчислювальну систему для моніторингу та впливу рівня диму, виявленого у домі.

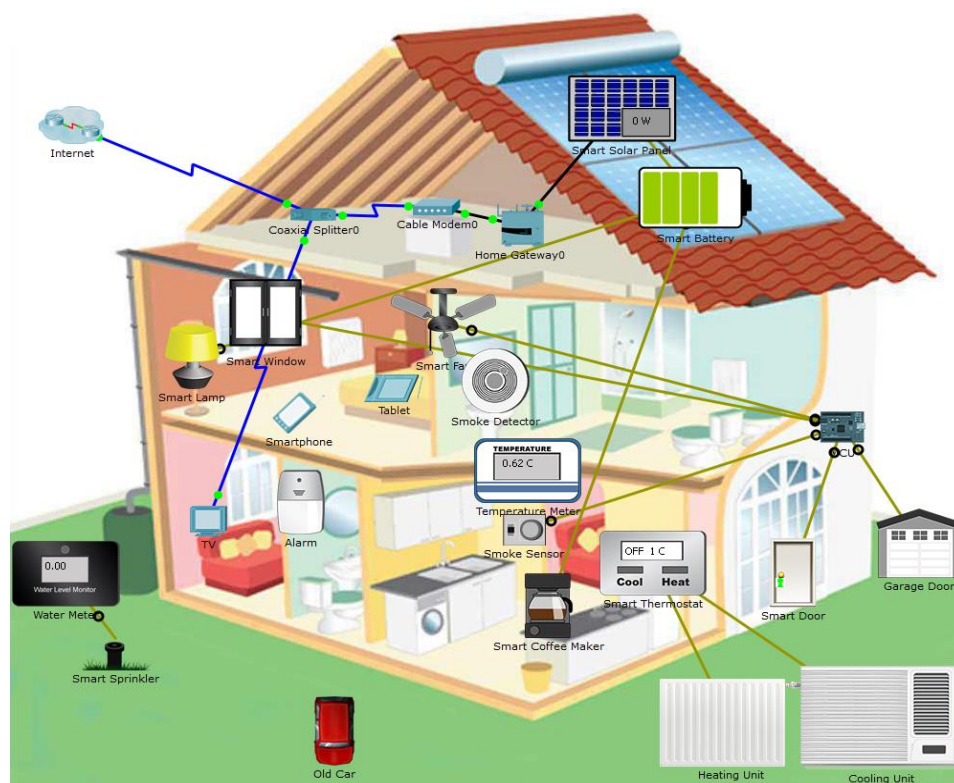


Рис. 4.1. Топологія розумної будівлі, обладнаної IoT пристроями.

Home Gateway - це концентратор і маршрутизатор для всіх внутрішніх пристроїв. Він також надає веб-інтерфейс, який дозволяє користувачам здійснювати моніторинг та керування різними розумними домашніми IoT пристроями. Зверніть увагу, що домашні пристрої можуть підключатися до домашнього шлюзу через бездротовий та / або дротовий зв'язок.

Зазвичай Інтернет-провайдери передають дані та відео за допомогою одного коаксіального кабелю. Починаючи з мансарди, коаксіальний спліттер використовується для відокремлення відеосигналу від сигналу даних.

Пристрої в розумному домі можна відслідковувати та управляти дистанційно через будь-який комп'ютер вдома. Оскільки всі розумні пристрої підключаються до домашнього шлюзу, на якому розміщено веб-інтерфейс, планшети, смартфони, ноутбуки та настільні комп'ютери і можуть використовуватися для взаємодії із розумними пристроями.

У прикладі розумного будинку найкращим варіантом було туманне обчислення. У прикладі смарт-будинку дані, отримані датчиками диму, оброблялись та використовувались для прийняття рішень щодо якості повітря в будинку. У цьому сценарії не потрібно було надсилати дані з датчиків у хмару для обробки. Хмарні обчислення можуть призвести до уповільнення часу відгуку, що може призвести до небезпеки для життя людей. Інша можлива проблема пов'язана з інтернет-зв'язком: якщо з'єднання з Інтернетом було втрачено, то нема можливості аналізувати ситуацію і реагувати на неї, внаслідок чого вся система могла б поставити життя людей в небезпеку. Зазначимо, що алгоритм прийняття рішень, наведений в даній роботі може бути вдосконалений інструментами нечіткої логіки [8].

Послідовність виконання роботи

Частина 1: Організація зв'язку в розумній будівлі

Крок 1.1: Вивчення пристроїв, що входять до складу розумного будинку

a. Два коаксіальні кабелі залишають коаксіальний спліттер у відображеній топології. Які пристрої підключаються до коаксіального кабелю?

b. Кабельний модем - це інтерфейс між мережею Інтернет-провайдера та домашньою мережею. На які пристрої підключається кабельний модем?

*Примітка. Packet Tracer використовує пунктирні пучки для зображення бездротових з'єднань, але це може бути незручним для читання, коли є забагато пристроїв. Щоб увімкнути це, перейдіть до **Options > Preferences > Hide Tab > uncheck Hide Wireless/Cellular Connection.***

c. Перерахуйте всі домашні пристрої, підключені до домашнього шлюзу

Крок 1.2: Взаємодія з Розумним будинком

d. Натисніть на **Планшет**. (Планшет розташований на ліжку в головній спальні).

e. Перейдіть до **Робочий стіл > Веб-браузер**.

f. В адресному рядку напишіть **192.168.25.1** і натисніть Enter. Це IP-адреса домашнього шлюзу.

g. Використовуйте **admin/admin** як ім'я користувача та пароль для входу в домашній шлюз.

h. Що відображається?

i. В даний час розумні двері відчинені (зелене світло на ручці дверей), але їх можна заблокувати віддалено. Натисніть розумні двері в браузері, щоб розгорнути цю опцію.

j. Натисніть **Lock**, щоб зачинити двері.

k. Чи зачинено двері? Звідки ви знаєте?

l. Натисніть **Unlock**, відчинити двері.

m. Натисніть детектор диму в браузері, щоб розгорнути розділ. Який рівень читання диму забезпечується детектором диму?

n. Чи можна контролювати датчик диму?

Розумними пристроями також можна керувати безпосередньо, представляючи фізичну взаємодію.

o. У межах логічної області роботи Packet Tracer утримуйте клавішу Alt і клацніть **Smart Coffee Maker**, щоб увімкнути або вимкнути.

Частина 2: Туманні обчислення в розумному будинку

MCU (Microcontroller Unit), доданий в розумний дім, використовується для контролю за рівнем диму, вимірним датчиком диму, і на основі програми приймає рішення, чи потрібно увімкнути вентиляцію. Якщо рівень монооксиду вуглецю вищий за 10,3 одиниці, MCU запрограмований на автоматичне відкриття вікна, передніх дверей, гаражних дверей та запуску вентилятора на високій швидкості. Ця дія є зворотною: зачиняються двері і вікна, зупиняється вентилятор, коли рівень окису вуглецю знизиться нижче 1 одиниці.

Крок 2.1: Запустіть класичний автомобіль

Власник тримає класичний автомобіль в гаражі і його потрібно запускати зрідка. Класичний автомобіль виробляє монооксид вуглецю, який підвищує рівень в приміщенні.

- p. Натисніть на **Tablet (планшет)** розташований на ліжку в головній спальні.
- q. Перейдіть до **Робочий стіл > Веб-браузер**.
- r. В адресному рядку введіть **192.168.25.1**. Це IP-адреса домашнього шлюзу.
- s. Використовуйте **admin/admin** як ім'я користувача та пароль для входу в домашній шлюз.
- t. Натисніть на детектор диму в розумному будинку; залиште це вікно відкритим, щоб ви могли стежити за рівнем диму.
- u. Запустіть двигун автомобіля, утримуючи клавішу Alt і натиснувши на класичний автомобіль.

Що відбувається з повітрям всередині будинку з автомобілем, що працює всередині гаража?

Що відбувається з повітрям усередині будинку після того, як MCU відкриває двері та вікно, і запускає вентилятор?

Чи закриває MCU двері та вікно і зупиняє вентилятор?

- v. Продовжуючи стежити за рівнями, зупиніть двигун класичного автомобіля, утримуючи клавішу Alt і натиснувши на класичний автомобіль.

Що відбувається з якістю повітря всередині будинку після зупинки двигуна?

Що відбувається з дверима, вікном та вентилятором?

Контрольні запитання

1. Поясніть переваги і недоліки туманних обчислень.
2. Дослідіть IoT кінцеві прилади в Packet Tracer і запропонуйте власні приклади розумних приладів в розумному будинкові (щоб оптимізувати його роботу). Які можливі рішення для людей з обмеженими можливостями (слабозрячі, слабочуючі, в інвалідних візках)?
3. Як організовано безпеку IoT системи розумного будинку?
4. Проведіть пошук в мережі Internet та запропонуйте механізми підвищення рівня безпеки IoT системи розумного будинку.

Лабораторна робота № 5

ЗАХИСТ ХМАРНИХ СЕРВІСІВ ІНТЕРНЕТУ РЕЧЕЙ В РОЗУМНІЙ БУДІВЛІ

Мета роботи: ознайомитися з основними сервісами хмарного інтернету речей та методами їх захисту, використовуючи симулятор Cisco Packet Tracer.

Обладнання: симулятор Cisco Packet Tracer.

Теоретичні відомості

Інтернет речей (IoT, Internet of Things) - це система датчиків і діючих механізмів, які керуються мікроконтролерами (MCU) через мережу Internet. Управлінські рішення приймаються програмованими мікроконтролерами на основі зібраної з датчиків інформації. Такими датчиками обладнують будівлі лікарень, лікарняних складів для оптимізації енергоспоживання, реалізації безпекових функцій. Лікарню, оснащену системою IoT, називатимемо розумною лікарнею. Також, системи датчиків використовують для безпосереднього моніторингу стану людини - в якості імплантів. Хмарні обчислення (Cloud computing, CC) є інструментом обробки зібраної з датчиків інформації. Взагалі CC – це доставка ІТ-ресурсів на вимогу користувача через мережу Інтернет. Користувач може отримати доступ до технологічних послуг, таких як обчислювальна потужність, сховище та бази даних за потреби від хмарного постачальника, наприклад, Amazon Web Services. Хмара використовується для резервного копіювання даних, аварійного відновлення, електронної пошти, розробки та тестування програмного забезпечення, аналітики великих даних, IoT даних. Моніторинг охорони здоров'я є однією з функцій пристроїв IoT, що передбачає збір та оцінку даних про пацієнтів протягом певного періоду часу. Моніторингові пристрої, які носить пацієнт (мережа датчиків тіла BSN, body sensor network), під'єднуються до Інтернету через спеціальний шлюз (на рисунку 4.1 це мікроконтролер Arduino та смартфон із відповідним застосунком). Шлюз поєднує сигнали від датчиків і

безпечно передає дані в хмару (рис. 4.1). IoT надає різні функції під'єднаним медичним пристроям. Датчики можна використовувати для відстеження місцезнаходження пристроїв IoT і моніторингу роботи пристроїв, щоб виявити проблеми та запобігти збоєм. У медичних пристроях (діючих механізмах) використовуються приводи, якими керує програмне забезпечення, щоб регулювати введення ліків, рідин і кисню.



Рис. 4.1. Система RPM (Remote Patient Monitoring) IoT.

Очевидно, що елементи такої системи потребують організації захисту від несанкціонованого втручання за допомогою надійного криптографічного алгоритму, інакше замість користі вони можуть принести шкоду, надавши кіберзлочинцям можливість для підриву інформаційної безпеки (оскільки пристрої із вбудованими комп'ютерами зберігають дуже багато інформації про свого власника, зокрема, можуть знати його точне місцезнаходження, доступ до такої інформації може допомогти зловмисникам здійснити злочин).

В даній лабораторній роботі розглянуто механізми організації захисту на прикладі складського приміщення розумної лікарні, де, як правило,

зберігаються ліки. Ліки вимагають специфічного температурного режиму зберігання, чіткого обліку, тому використано IoT безпекові системи із хмарними сервісами. (Рис.4.2).

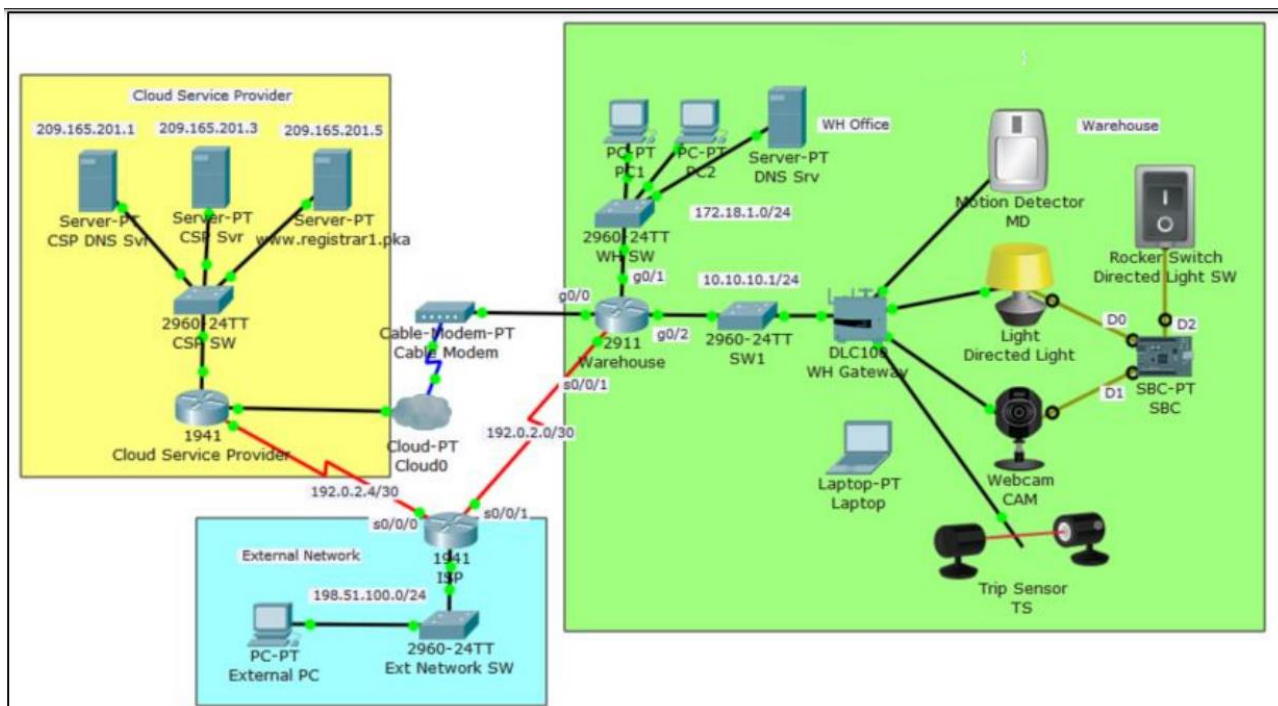


Рис.4.2. Топологія системи IoT складського приміщення розумної лікарні.

IoT пристрої безпеки (вебкамера та детектор руху) стежать за дверима та вікнами коли склад закритий. Якщо зловмисника буде виявлено, увімкнеться світло і веб-камери почнуть запис. Для цього в симуляторі Packet Tracer на реєстраційному сервері потрібно виконати такі дії:

- 1) зареєструвати чотири пристрої IoT складського приміщення розумної лікарні: детектор руху, спрямоване світло, веб-камера та датчик від'єднання.
- 2) додати умови, щоб при активації датчика руху **MD** (Motion Detector, датчик руху, рис. 4.2) або датчика відключення **TS** (Trip Sensor, датчик від'єднання рис. 4.2), увімкнулось спрямоване світло **Directed Light** та веб-камера **CAM**.

Послідовність виконання роботи

Крок 1. Реєстрація IoT-пристрої на сервері реєстрації

1.1. Доєднання користувача до сервера реєстрації www.registrar1.pka з надійним паролем (підготовка до безпосередньої реєстрації)

1.1.1. Використовуйте ПК у офісі WH (Рис. 4.2). У вкладці *Desktop* відкрийте веб-браузер, введіть www.registrar1.pka та оберіть *Go*. З'явиться вікно реєстрації.

1.1.2. Натисніть *Sign up now* та створіть ваш власний акаунт з надійним паролем (переконайтеся, що пароль містить не менше 8 символів в комбінації з великих літер, малих символів та цифр).

1.2. Безпосередня реєстрація пристроїв IoT на сервері реєстрації.

1.2.1. У межах складу натисніть на детектор руху. У вкладці *Config* оберіть *Remote Server* у розділі сервера IoT. Введіть www.registrar1.pka як адресу сервера та натисніть *Connect*. Введіть ім'я користувача/пароль, який ви щойно створили. Чи з'являється детектор руху на сервері реєстрації?

1.2.2. Повторіть кроки з пункту 1.2.1, щоб зареєструвати датчик світла, веб-камери та датчик відключення.

Крок 2. Налаштування умов на сервері реєстрації

Додаємо умови на сервері реєстрації, щоб при активації датчика руху або датчика руху, спрямоване світло та веб-камера були ввімкнені.

2.1. Заходимо на сервер реєстрації, використовуючи щойностворені ім'я користувача та пароль. Чи бачите ви чотири пристрої IoT у вигляді списку?

2.2. Натисніть *Conditions* і додайте наступні три умови:

2.2.1. Назвіть умову *LightsOn1*, якщо статус **MD** - "Увімкнено", тоді встановіть статус направленого світла на "Увімкнено" та встановіть статус **SAM** на "Увімкнено".

2.2.2. Назвіть умову *LightsOn2*, якщо **TS**-статус - "Увімкнено", тоді встановіть статус напрямленого світла **Directed Light** на "Увімкнено" та встановіть **SAM**-статус на "Увімкнено".

2.2.3 Назвіть умову *LightsOff*, якщо обидва **MD**-статуси "Увімкнено" є хибними та **TS**-статус "Увімкнено" також є хибним, потім

встановіть *Directed Light*-статус на "Вимкнено" AND та CAM-статус "Увімкнено" на хибний.

2.2.4. Протестуйте умови. Утримуйте клавішу ALT і перемістіть мишу над детектором руху. Чи увімкнено режими освітлення та веб-камеру?

Відсуньте мишку і чекайте декілька секунд. Чи вимкнено режими освітлення та веб-камеру?

Контрольні запитання

1. Що таке розумна лікарня?
2. В чому полягає перевага використання хмарних сервісів в медичному IoT?
3. Як відбувається реєстрація IoT пристроїв на сервері?
4. Поясніть, будь ласка, як прописуються умови ввімкнення веб-камери та світла?
5. Проведіть пошук в мережі Інтернет та запропонуйте свої ідеї для покращення безпеки IoT розумної лікарні.

Лабораторна робота № 6

ЕВОЛЮЦІЯ БЕЗПЕКОВИХ ОПЦІЙ В ПРОТОКОЛАХ WiFi ЗВ'ЯЗКУ

Мета роботи: ознайомитися з основними безпековими опціями WiFi зв'язку, використовуючи симулятор Cisco Packet Tracer.

Обладнання: симулятор Cisco Packet Tracer.

Теоретичні відомості

В попередніх лабораторних роботах було розглянуто мережі інтернету речей та хмарні сервіси для збору, збереження та аналізу медичної інформації з метою оптимізувати допомогу пацієнтам. Передача даних в таких мережах відбувається по WiFi бездротових протоколах, тому сучасному лікареві варто розуміти механізми захисту цього інформаційного каналу зв'язку. Очевидно, що для злочинців незахищені канали WiFi зв'язку не просто можуть бути джерелом конфіденційної інформації, але і інструментом безпосередньої реалізації атаки на пацієнта. Наприклад, при використанні імплантованої інсулінової помпи (для підтримки стабільного рівня інсуліну в крові), злочинець може, перехопивши пароль, поміняти налаштування такого імпланта з усіма витікаючими наслідками.

В даній лабораторній роботі студенти розглянуть три різні протоколи WiFi зв'язку: від простого із слабким рівнем захисту до складнішого і досконалішого. Перший протокол WEP (Wired Equivalent Privacy, WEP) використовує постійний ключ для шифрування. Керування ключами у WEP не передбачено, тому кількість людей, яким відомий один і той самий ключ, буде постійно зростати, оскільки всі учасники його використовують. Цей протокол ми застосуємо на об'єкті **Healthcare at Home** (рис. 5.1), тобто домашній WiFi.

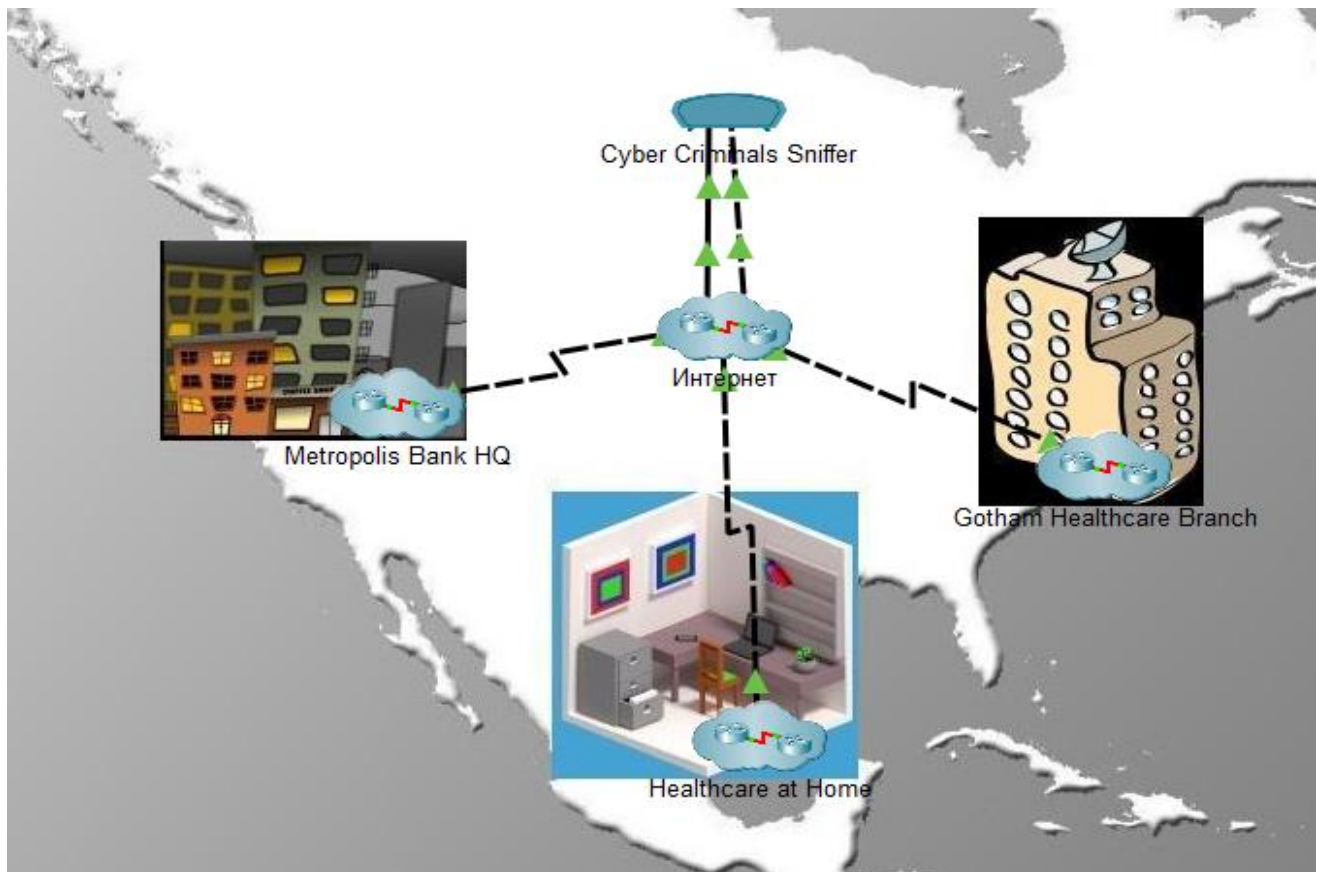


Рис. 5.1. Логічна схема розміщення об'єктів: Healthcare at Home, Gotham Healthcare Branch та Metropolis Bank HQ.

Другий протокол WPA2 PSK (Wi-Fi Protected Access, WPA) є досконалішою версією попереднього протоколу з більш надійними алгоритмами шифрування. WPA2 PSK будемо налаштовувати на **Gotham Healthcare Branch**, тобто у будівлі лікарні (рис. 5.1).

Третій протокол WPA2 RADIUS

також є вдосконаленою версією попереднього протоколу, але тут уже додано інфраструктуру відкритих ключів - кожен користувач має своє ім'я та пароль (а не один для всіх користувачів постійний ключ). WPA2 RADIUS застосуємо на об'єкті **Metropolis Bank HQ**, тобто у банку, через який здійснюються фінансові операції пацієнтів і де зберігається дуже чутлива інформація.

Послідовність виконання роботи

1. Налаштування WEP на об'єкті Healthcare at Home

1.1. Налаштування ідентифікатора SSID бездротової мережі.

- a. Натисніть на об'єкт **Healthcare at Home** і виберіть **PC0**.
- b. Виберіть вкладку **Desktop**. Натисніть **Command Prompt**. У командному рядку введіть команду **ipconfig**.

PC> **ipconfig**

Link-local IPv6 Address.....: FE80::20B:BEFF:FEB4:1262

IP Address.....: 10.44.3.100

Subnet Mask.....: 255.255.255.0

Default Gateway.....: 10.44.3.1

Яка IP адреса у шлюза по замовчуванню?

- c. Перейдіть до застосунку **Web Browser** (Браузер) і введіть IP-адресу шлюзу. Введіть **admin** в якості імені користувача і пароля при появі запиту. Натисніть **OK**.
- d. **Wireless Router** є шлюзом за замовчуванням для цієї мережі. Натисніть на вкладку **Wireless** (Бездротова мережа).
- e. Змініть **SSID** з **DefaultWIFI** на **Home**.
- f. Увімкніть передачу ідентифікатора SSID. Виберіть для цього **Broadcast** (Передавати).
- g. Натисніть **Save Settings** (Зберегти параметри). Натисніть **Continue**.

1.2. Налаштування захисту бездротової мережі.

- a. Виберіть бездротовий маршрутизатор **Wireless Router** і

натисніть **Wireless** > **Wireless Security** (Бездротова мережа > Захист бездротової мережі).

- b. В спадаючому меню Security Mode (Режим захисту) виберіть **WEP**.
- c. Встановіть для параметру шифрування Encryption значення 40/64-біт і введіть ключ **0123456789** у якості Key 1.
- d. Натисніть кнопку **Save Settings** (Зберегти параметри).
Натисніть **Continue**.

Захист WEP і ключ 0123456789 не є надійними. Чому алгоритм WEP не рекомендується використовувати для захисту бездротових мереж?

1.3. Під'єднання клієнтських пристроїв.

- a. Відкрийте об'єкт **Healthcare at Home** і виберіть ноутбук **Dave**.
- b. Перейдіть на вкладку **Desktop** (Робочий стіл) і натисніть **PC Wireless** (Бездротовий зв'язок).
- c. Перейдіть на вкладку **Connect** (Під'єднатись) і потім натисніть **Refresh** (Оновити).
- d. Виберіть бездротову мережу з іменем **Home** і натисніть **Connect**.
- e. Введіть ключ **0123456789** у якості WEP Key 1 і натисніть **Connect**.
- h. Повторіть кроки **a - e** для ноутбука **Mary**.

2. Налаштування WPA2 PSK на об'єкті Gotham Healthcare Branch

2.1. Налаштування ідентифікатора SSID бездротової мережі.

- a. Відкрийте об'єкт **Gotham Healthcare Branch** і виберіть **PC1**.
- b. Виберіть вкладку **Desktop** . Натисніть **Command Prompt**. У командному рядку введіть команду **ipconfig**.

Запишіть IP адресу для шлюзу по замовчуванню:

-
- c. Перейдіть до застосунку **Web Browser** (Браузер) і введіть IP-адресу шлюзу. Введіть **admin** в якості імені користувача і пароля при появі запиту. Натисніть **OK**.
 - d. Натисніть на вкладку **Wireless** (Бездротова мережа).
 - e. Змініть ідентифікатор **SSID** з **DefaultWIFI** на **BranchSite**.
 - f. Змініть стандартний канал Standard Channel на **6 – 2.437GHz**.
 - g. Увімкніть передачу ідентифікатора SSID. Для цього виберіть варіант **Broadcast** (Передавати).
 - h. Натисніть кнопку **Save Settings** (Зберегти параметри).
Натисніть **Continue**.

2.2 Налаштування захисту бездротової мережі.

- a. Виберіть бездротовий маршрутизатор Wireless Router і натисніть **Wireless > Wireless Security** (Бездротова мережа > Захист бездротової мережі).
- b. В спадаючому меню Security Mode (Режим захисту) виберіть **WPA2 Personal**.
- c. Залиште параметри шифрування Encryption значення по замовчуванню **AES** та введіть пароль **ciscosecure**.
- d. Натисніть кнопку **Save Settings** (Зберегти параметри).
Натисніть **Continue**.

2.3. Під'єднання клієнтських пристроїв.

- a. Відкрийте об'єкт **Gotham Healthcare Branch** і виберіть комп'ютер **Tim**.
- b. Перейдіть на вкладку **Desktop** (Робочий стіл) і натисніть **PC Wireless** (Бездротовий зв'язок).

- c. Перейдіть на вкладку **Connect** (Під'єднатись) і потім натисніть **Refresh** (Оновити).
- d. Виберіть бездротову мережу з іменем **BranchSite** і натисніть **Connect**.
- e. Введіть PSK-ключ **ciscosecure** і натисніть **Connect**.
- f. Повторіть кроки **a - e** для комп'ютера **Mike**.

3. Налаштування WPA2 RADIUS на об'єкті Metropolis Bank HQ

1. Налаштування ідентифікатора SSID бездротової мережі.

- a. Відкрийте об'єкт **Metropolis Bank HQ** і виберіть **Sally**.
- b. Перейдіть до застосунку **Web Browser (Браузер)** і введіть IP адресу бездротового маршрутизатора (**10.44.1.251**). Введіть **admin** в якості імені користувача і пароля при появі запиту. Натисніть **OK**.
- c. Натисніть на вкладку **Wireless** (Бездротова мережа).
Змініть **SSID** з **DefaultWIFI** на **HQ**.
- d. Змініть значення параметру стандартного каналу
Standart Channel на **11 – 2.462GHz**.
- e. Увімкніть передачу ідентифікатора SSID. Для цього виберіть варіант **Broadcast** (Передавати).
- f. Натисніть кнопку **Save Settings** (Зберегти параметри).
Натисніть **Continue**.

3.2. Налаштування захисту бездротової мережі.

- a. Виберіть бездротовий маршрутизатор **Wireless Router** і натисніть **Wireless > Wireless Security** (Бездротова мережа > Захист бездротової мережі).
- b. В спадаючому меню **Security Mode** (Режим захисту) виберіть **WPA2-Enterprise**.

- c. Встановіть для параметру шифрування Encryption значення **AES** і введіть наступні облікові дані сервера RADIUS:

RADIUS SERVER IP (IP-адреса сервера RADIUS): **10.44.1.252**

Shared Secret (Спільний секретний ключ): **ciscosecure**
- d. Натисніть кнопку **Save Settings** (Зберегти параметри).
Натисніть **Continue**.

3.3. Налаштування сервера RADIUS.

- a. Відкрийте об'єкт **Metropolis Bank HQ** і виберіть сервер **NTP/AAA**.
- b. Перейдіть на вкладку **Services** (Служби) і виберіть розділ **AAA**.
- c. Введіть наступну інформацію в області **Network Configuration** (Конфігурація мережі):

Client Name (Ім'я клієнта): **HQ**

Client IP (IP-адреса клієнта): **10.44.1.251**

Secret (Ключ): **ciscosecure**

ServerType (Тип сервера): **RADIUS**
- d. Натисніть **Add** (Додати).
- e. Введіть наступну інформацію в області **User Setup** (Параметри користувачів) і натисніть кнопку **Add**, щоб додати нове ім'я користувача:

Username: **bob** Password: **secretninjabob**

Username: **phil** Password: **philwashere**

3.4. Підключення клієнтських пристроїв.

- i. Відкрийте об'єкт **Metropolis Bank HQ** і виберіть комп'ютер **Bob**.
- j. Перейдіть на вкладку **Desktop** (Робочий стіл) і натисніть **PC Wireless** (Бездротовий зв'язок).

- k. Перейдіть на вкладку **Profiles** (Профілі) і потім натисніть **New** (створити новий).
- l. Назвіть профіль **RADIUS** і натисніть **OK**.
- m. Натисніть **Advanced Setup** (розширені налаштування).
- n. Введіть ім'я бездротової мережі **HQ** і натисніть **Next**.
- o. Не змінюючи налаштувань мережі знову натисніть **Next**.
- p. У спадаючому меню Wireless Security виберіть режим захисту **WPA2-Enterprise** і натисніть **Next**.
- q. Введіть ім'я користувача **bob** і пароль **secretninjabob**. Натисніть **Next**.
- r. Натисніть **Save** (Зберегти) і потім **Connect to Network** (Під'єднатися до мережі).
- s. Комп'ютер **Bob** під'єднається автоматично.
- t. Повторіть кроки **a-j** для ноутбука **Phil**, використовуючи аутентифікаційну інформацію з кроку 3e.

Чому у великій організації доцільніше застосувати режим WPA2 RADIUS замість WPA2 PSK? _____

Контрольні запитання

1. Які є протоколи WiFi зв'язку? Назвіть особливості кожного з протоколів.
2. Який протокол WiFi зв'язку є найбільш захищеним?
3. Запропонуйте власні рішення для покращення рівня безпеки WiFi зв'язку – не соромтеся спитати пораду у чату GPT.
4. Чи має технологія Blockchain потенціал застосування для вдосконалення безпеки WiFi зв'язку ?

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

Основна література

1. Snegursky A.V., Panait T.I., Puga H.D., Snegurskaya T.A., Rizak V.M. Medical and biological physics: Part I: Metrology, biometrics, mechanics and molecular physics. Methodical laboratory work guidelines for medical students. — Uzhhorod, 2015. — 80 p.
2. Телемедицина та комп'ютерні мережі: Лабораторний практикум у Cisco Packet Tracer»: навч. посіб. для студ. спеціальності 163 «Біомедична інженерія» / уклад. В.А. Данілова, В.В. Шликов; КПІ ім. Ігоря Сікорського.– Київ: КПІ ім. Ігоря Сікорського», 2021. – 73 с.
3. Програмування пристроїв Інтернету речей: лабораторний практикум [Електронний ресурс] : навч. посіб. для студ. спеціальності 121 «Інженерія програмного забезпечення» (освітня програма «Програмне забезпечення комп'ютерних та інформаційно-пошукових систем») / КПІ ім. Ігоря Сікорського ; уклад.: Л.М. Олещенко, Я.В. Хіцко.– Київ : КПІ ім. Ігоря Сікорського, 2019. – 47 с.
4. Introduction to IoT (Cisco Networking Academy) // Електронний ресурс. Режим доступу: <https://www.netacad.com>.
5. IoT Fundamentals Connecting Things (Cisco Networking Academy) // Електронний ресурс. Режим доступу: <https://www.netacad.com>.
6. Олещенко, Л. М. Проєктування та розроблення мережевого програмного забезпечення. Лабораторний практикум [Електронний ресурс] : навчальний посібник для студентів, які навчаються за спеціальністю 121 «Інженерія програмного забезпечення» (освітня програма «Інженерія програмного забезпечення мультимедійних та інформаційно-пошукових систем») / Л. М. Олещенко ; КПІ ім. Ігоря Сікорського. – Електронні текстові данні. – Київ : КПІ ім. Ігоря Сікорського», 2023. – 108 с.
7. Young-Sik Jeong, Jong Hyuk Park. IoT and Smart City Technology:

Challenges, Opportunities, and Solutions // Journal of Information Processing Systems. Volume 15, No 2 (2019), pp. 233 – 238.

8. Polishchuk V. Evaluation of start-up projects in conditions of risk and uncertainty. – Uzhhorod: Publishing house "FOP Sabov AM", 2021. – 120 p. ISBN 978-617-7798-49-0

Допоміжна література

1. Rejeb A., Rejeb K., Simske S., Treiblmaier H., Zailani S. The big picture on the internet of things and the smart city: a review of what we know and what we need to know// Internet of Things, 2022. - Volume 19. – P. 100565
2. Pierfrancesco Bellini P., Pantaleo G. Special Issue on the Internet of Things (IoT) in Smart Cities// Appl. Sci. 2023. - 13(7), 4392. <https://doi.org/10.3390/app13074392>

Інформаційні ресурси в мережі Інтернет

1. Course: IoT and Arduino Experiment. Lecturer: Sung Geumyoung. 2020. Handong Global University. [Електронний ресурс]. – Режим доступу: <https://www.hufocw.org/Course/767>
2. Course: Smart city and Eco Tourism. Lecturer: Seo Ducksu. 2020. Handong Global University. [Електронний ресурс]. – Режим доступу: <https://www.hufocw.org/Course/675>