МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ФРАНКА

Факультет прикладної математики та інформатики
(повне найменування назва факультету)

кібербезпеки
(повна назва кафедри)

Дипломна робота

Розробка моделі захисту інформаційних потоків у самоорганізованих транспортних мережах (VANET)

Виконав: студент групи ПМК-42с
спеціальності
125 «Кібербезпеки»
(шифр і назва спеціальності)

(підпис) Ващук О.В.
(прізвище та ініціали)

Керівник (підпис) Комар К.В.
(прізвище та ініціали)

Науковий консультант (підпис) Вайганг Г.О.
(прізвище та ініціали)

Рецензент (підпис) О. Є. Гларіонов
(прізвище та ініціали)

2023

ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ФРАНКА

Факультет Прикладної математики та інформатики
Кафедра Кібербезпеки
Спеціальність: 125 «Кібербезпека»
«шифр і назва»

«ЗАТВЕРДЖУЮ»
Завідувач кафедри _____

"31 "серпня 2022 року

ЗАВДАННЯ

на кваліфікаційну бакалаврську роботу студента
Ващука Олександра Валентиновича
(прізвище, ім'я, по батькові)

1. **Тема роботи**: Розробка моделі захисту інформаційних потоків у самоорганізованих транспортних мережах (VANET)

Керівник роботи асистент Комар К.В., науковий консультант Вайганг Г.О. затверджені наказом університету від «13» вересня 2021 року № 15

2. **Строк подання студентом роботи** «13» червня 2023 року
3. **Вихідні дані до роботи:**

4. **Зміст пояснювальної записки (перелік питань, які потрібно розробити)**
1. Огляд особливостей самоорганізованих транспортних мереж та їх завдання
2. Дослідження структури та архітектури мережі VaNet
3. Кібербезпека мереж VANET: загрози , вразливості, атаки
4. Моделювання бездротових сенсорних мереж

5. **Перелік графічного матеріалу:**

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання **31 серпня 2022 р.**

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломної роботи	Строк виконання етапів роботи	Примітка
1	Уточнення постановки завдання	21.03.2023	
2	Аналіз літератури	28.03.2023	
3	Обґрунтування вибору рішення	31.03.2023	
4	Збір даних	07.04.2023	
5	Опис особливостей IP-NOC VINET	18.04.2023	
6	Дослідження структури VINET	28.04.2023	
7	Опис кібербезпеки мережі VINET	12.05.2023	
8	Моделювання бездротових мереж	22.05.2023	
9	Оформл. та здача пояснюв. записк. та граф	06.06.2023	
10	Отримання рецензій	10.06.2023	
11	Подання роботи на кафедру	12.06.2023	
12	Захист ВЕК	16.06.2023	

Студент _____ (підпис) Ващук О.В. (ініціали, прізвище)

Керівник роботи _____ (підпис) Комар К.В. (ініціали, прізвище)

РЕФЕРАТ

Пояснювальна записка дипломного проекту складається зі вступу, чотирьох розділів, що містять 33 рисунків, висновків та списку використаних джерел з 44 найменувань. Загальний обсяг роботи становить 90 сторінок.

Об’єкт дослідження: безпека самоорганізованих мереж VaNet.

Метою даної роботи є дослідження елементів захисту мереж VaNet та визначення загроз, які можуть вплинути на їх безпеку.

У першому розділі проводиться детальний аналіз основних концепцій та принципів самоорганізованих транспортних мереж. Розглядаються типи таких мереж, зокрема Ad-Hoc, Mesh та MANET, а також їхні переваги та недоліки.

У другому розділі проводиться аналіз розташування транспортних засобів та інфраструктури в мережі VaNet. Розглядаються різні форми структури мережі, такі як меш-мережі, мережі з точками доступу та інші.

У третьому розділі проводиться дослідження загроз, вразливостей та атак, які можуть впливати на мережі VANET. Аналізуються різні типи атак, які можуть бути спрямовані на мережі VANET, включаючи атаки на конфіденційність, цілісність та доступність даних. Розглядаються методи захисту та протидії таким атакам.

У четвертому розділі проводиться дослідження моделей та методів моделювання бездротових сенсорних мереж. Розглянута прикладна розробка мережі "розумного" міста, що використовує мережу з використанням пристроїв IoT, які є структурними елементами системи V2I (Vehicle-to-Infrastructure).

Ключові слова: VANET, ТОПОЛОГІЇ МЕРЕЖ, MESH, MANET, АРХІТЕКТУРА, ПРОТОКОЛИ, ЗАГРОЗИ, БЕЗПЕКА.

ABSTRACT

The explanatory note of the diploma project consists of an introduction, three chapters containing 33 figures, conclusions and a list of 44 references. The total volume of the work is 90 pages.

Object of study: security of self-organized VaNet networks.

The **purpose** of this paper is to study the security elements of VaNet networks and identify threats that may affect their security.

The first section provides a detailed analysis of the basic concepts and principles of self-organized transport networks. The types of such networks, such as Ad-Hoc, Mesh, and MANETs, as well as their advantages and disadvantages, are discussed.

The second section analyzes the location of vehicles and infrastructure in a VaNet network. Different forms of network structure are considered, such as mesh networks, networks with access points, and others.

In the third section, the threats, vulnerabilities, and attacks that can affect VANETs are studied. Different types of attacks that can be directed at VANETs are analyzed, including attacks on data confidentiality, integrity, and availability. Methods of protecting and counteracting such attacks are considered.

The fourth chapter studies models and methods of modeling wireless sensor networks. An applied development of a smart city network using IoT devices, which are the structural elements of the V2I (Vehicle-to-Infrastructure) system, is considered.

Keywords: VANET, NETWORK TOPOLOGIES, MESH, MANET, ARCHITECTURE, PROTOCOLS, THREATS, SECURITY.

ЗМІСТ

СПИСОК СКОРОЧЕНЬ

MANET	– Mobile Ad Hoc Network
OBU (On Board Unit)	– спеціалізовані телекомунікаційні модулі встановлені на ТЗ
RSU (Roadside Unit)	– інфраструктурні базові станції
V2I	– Vehicle 2 Infrastructure
V2V	– Vehicle 2 Vehicle
VANET	– Vehicular Ad Hoc Network
VRC	– Vehicle to Roadside Communication
IT	– інформаційні технології
ITC	– інтелектуальні транспортні системи

ВСТУП

Актуальність. Сучасний розвиток технологій сприяє створенню нових підходів до організації транспортних систем. Одним з таких підходів є використання самоорганізованих транспортних мереж (VaNet - Vehicular Ad Hoc Network). VaNet - це бездротова мережа, яка забезпечує зв'язок між рухомими транспортними засобами та іншими елементами інфраструктури, такими як дорожні знаки, світлофори та інші транспортні системи. Вона має великий потенціал у поліпшенні безпеки на дорогах, забезпеченні ефективного управління трафіком та наданні нових послуг для користувачів.

Сучасний рівень розвитку бездротових технологій передачі даних дійсно дозволяє створювати та використовувати сучасні сервіси з майже будь-якої точки планети. В рамках автомобільного транспорту така технологія втілилася у створенні та впровадженні мереж автомобільного транспорту VANET (Vehicle Ad-Hoc Networks).

VANET є формою бездротової мережі, в якій автомобілі та інші транспортні засоби взаємодіють між собою та з придорожною інфраструктурою, обмінюючи інформацію про рух, безпеку, дорожні умови та інші важливі дані. Ця мережа забезпечує покращення безпеки, ефективності та комфорту на дорогах.

Застосування VANET включає такі можливості:

- Виявлення і попередження про аварійні ситуації та небезпеки на дорозі.
- Оптимізація руху автомобілів, зокрема управлінням сигналізацією світлофорів та регулюванням потоку транспорту.
- Покращення системи публічної безпеки, включаючи розшук викрадених автомобілів та трасування викрадених транспортних засобів.
- Передача інформації про парковки, сервіси, туристичні об'єкти та інші корисні дані для водіїв та пасажирів.

Використання VANET також відкриває можливості для автономних та з'єднаних автомобілів, дозволяючи їм взаємодіяти між собою та з інфраструктурою, обмінюючись даними про шляхи, рух, стан доріг та інше.

Проте впровадження мереж автомобільного транспорту VANET також вносить виклики, пов'язані з безпекою, конфіденційністю даних, надійністю комунікацій та управлінням мережею. Тому важливо розробляти та впроваджувати відповідні механізми і стандарти для забезпечення захисту та ефективності цих мереж.

Захист автомобільних самоорганізованих мереж (VANETs) є надзвичайно актуальним і важливим аспектом розвитку транспортних систем. Оскільки VANETs використовують бездротовий зв'язок для обміну інформацією між автомобілями та придорожньою інфраструктурою, вони можуть стати цільовою точкою для різноманітних кібератак та зловмисних дій.

Оскільки VANETs є життєво важливою складовою інтелектуальних транспортних систем, безпека їх функціонування має велике значення. Ефективний захист VANETs є вирішальним для забезпечення безпеки та ефективності автомобільних транспортних систем.

Об’єкт дослідження: безпека самоорганізованих мереж VaNet.

Метою даної роботи є дослідження елементів захисту мереж VaNet та визначення загроз, які можуть вплинути на їх безпеку.

Для вирішення поставленої мети були сформовані наступні завдання:

- розглянути види та принципи роботи самоорганізованих мереж Ad-Hoc, зокрема мереж Mesh і MANET;
- дослідити структуру та архітектуру мережі VaNet, включаючи комунікаційні протоколи та механізми маршрутизації;
- визначити загрози та виклики, з якими стикаються мережі VANET, зокрема в контексті автономних транспортних систем;
- проаналізувати різні засоби моделювання бездротових сенсорних мереж, зокрема їх переваги та обмеження;
- розглянути прикладну розробку мережі "розумного" міста як інструменту взаємодії між транспортними засобами та інфраструктурою.

РОЗДІЛ 1.
ОГЛЯД ОСОБЛИВОСТЕЙ САМООРГАНІЗОВАНИХ ТРАНСПОРТНИХ МЕРЕЖ ТА ЇХ ЗАВДАННЯ

1.1 Основні поняття самоорганізованих транспортних мереж VaNet

Автомобільні самоорганізовані мережі (VANETs) є ключовою частиною інтелектуальних транспортних систем (ITC) і використовують технології бездротового зв'язку для забезпечення зв'язку між транспортними засобами та придорожньою інфраструктурою.

VANETs використовуються з метою поліпшення безпеки на дорозі, покращення ефективності руху, забезпечення комфорту для водіїв і пасажирів, а також зменшення впливу транспорту на навколишнє середовище. Ці мережі дозволяють транспортним засобам обмінюватися інформацією про дорожню ситуацію, перешкоди на дорозі, дорожні знаки, сигнали світлофорів та інші важливі дані [1].

Однією з ключових характеристик VANETs є їх самоорганізація. Транспортні засоби, обладнані вбудованою бездротовою технологією, можуть автоматично формувати мережу і обмінюватися інформацією без потреби централізованого управління. Це робить їх гнучкими і відповідними для широкого спектру застосувань у сфері транспорту.

Забезпечення безпеки в VANETs є однією з найважливіших задач. Оскільки транспортні засоби обмінюються критичною інформацією, такою як повідомлення про аварії, небезпечні дорожні умови або інші нагальні ситуації, необхідно забезпечити конфіденційність, цілісність та доступність цієї інформації. Для цього використовуються різні криптографічні протоколи, аутентифікація транспортних засобів, системи виявлення вторгнень та інші заходи безпеки [2].

Крім того, існує потреба в стандартизації і регулюванні VANETs для забезпечення сумісності та взаємодії між різними системами. Нормативні акти і стандарти допомагають створювати єдині правила і вимоги, які сприяють розвитку та використанню автомобільних самоорганізованих мереж.Одне з

Висновки до розділу 1

В цьому розділі розглянули основні аспекти самоорганізованих транспортних мереж VaNet і мереж Ad-Hoc, а також технології Wi-Fi, що використовуються в цих мережах.

Самоорганізовані транспортні мережі VaNet є бездротовими мережами, які забезпечують спілкування між транспортними засобами та придорожніми блоками. Вони мають характеристики бездротового зв'язку, мобільності, самоорганізації та підтримки реального часу.

Мережі Ad-Hoc, такі як Mesh і MANET, є підтипами самоорганізованих мереж і мають свої властивості та принципи роботи. Мережі Mesh мають гнучку структуру, а MANET є мобільними мережами без потреби в попередній інфраструктурі.

Технології Wi-Fi, зокрема стандарти IEEE 802.11p, є важливими для забезпечення бездротового зв'язку у VaNet. Ці стандарти визначають протоколи та механізми для безпеки, мобільності та якості обслуговування в мережах VaNet.

Загальною метою нашого дослідження є розуміння та розвиток самоорганізованих транспортних мереж та їх застосувань. Цей огляд дав нам основні поняття і фундаментальні знання, які стануть основою для подальшого дослідження та розробки в цій області.

РОЗДІЛ 2.
ДОСЛІДЖЕННЯ СТРУКТУРИ ТА АРХІТЕКТУРИ МЕРЕЖІ VANET

3.1 Структура мережі VaNet та її особливості

Автомобільна мережа (VaNet) - це спеціальна самоорганізована мережа, яка використовується для допомоги транспортній системі в різних додатках, таких як безпека дорожнього руху, управління дорожнім рухом, контроль швидкості, інформаційно-розважальні послуги на транспортних засобах, допомога безпілотним автомобілям тощо.

Мережа VaNet (Vehicle Ad-hoc Network) є самоорганізованою транспортною мережею, яка забезпечує бездротовий зв'язок між транспортними засобами і дорожньою інфраструктурою. Основними особливостями мережі VaNet є специфіка вузлів мережі (транспортних засобів), динамічність та мобільність.

Структура мережі VaNet базується на принципах ад-гок мереж (ad-hoc networks) та мереж мобільних агентів. Транспортні засоби, обладнані вбудованими пристроями бездротового зв'язку, виступають в якості вузлів мережі. Вони можуть бути обладнані різними типами пристроїв, такими як датчики, GPS-приймачі, камери та інші, для збору та передачі різноманітної інформації.

Однією з особливостей мережі VaNet є її динамічність. Транспортні засоби можуть приєднуватися до мережі або виходити з неї на ходу, що створює постійні зміни в топології мережі. Це вимагає від мережевих протоколів і алгоритмів маршрутизації гнучкості і ефективності, щоб забезпечити надійний зв'язок у змінних умовах руху.

Ще одною особливістю мережі VaNet є її мобільність. Транспортні засоби постійно пересуваються, що впливає на сигнали бездротового зв'язку. Перешкоди, такі як будівлі, дерева або інші транспортні засоби, можуть впливати на якість зв'язку. Тому необхідні ефективні алгоритми маршрутизації та управління ресурсами, які можуть адаптуватися до змін у мережі та умовах руху.

Структура мережі VaNet передбачає наявність базових станцій дорожньої інфраструктури, які забезпечують збір інформації від транспортних засобів і розповсюджують її в мережі. Ці базові станції можуть бути розташовані на світлофорах, дорожніх знаках, смугах аварійної зупинки тощо. Вони є важливим елементом інфраструктури VaNet, оскільки забезпечують збір та обробку інформації для покращення безпеки та ефективності руху.

Для підтримки цих додатків з'явилося кілька варіантів автомобільних мереж, які керуються сучасними технологіями, такими як п'яте покоління (5G), Інтернет речей (IoT), програмно-визначені мережі (SDN), периферійні обчислення та хмарні обчислення. Впровадження передових технологій вимагає більш інтелектуальних рішень для вирішення проблем, що виникають через різноманітну природу автомобільних конструкцій. Автомобільна промисловість усвідомлює необхідність нових протоколів і методів, сумісних з новими мережевими тенденціями і варіантами.

Традиційна архітектура автомобільних спеціальних мереж (VANET), що використовуються для надання допомоги автономним і неавтономним транспортним засобам, складається з бортового пристрою (OBU), периферійних пристроїв, придорожнього блоку (RSU), централізованих контролерів і довіреного органу (TA).

Автомобільна мережа зв'язується з периферійною мережею, яка, в свою чергу, підключена до магістральної мережі через дротовий або бездротовий носій. Передача даних відбувається між транспортними засобами та різними рівнями оренди мереж, що призводить до різних типів зв'язку [13], тобто vehicle-to-vehicle (V2V), vehicle-to-RSU (V2R), infrastructure-to-infrastructure (I2I), vehicle-to-infrastructure (V2I) та багато іншого. Покращені можливості підключення та збільшення кількості каналів зв'язку та точок доступу призвели до кількох проривів. У той же час вони ставлять ряд проблем, які необхідно враховувати при розробці автомобільних рішень, важливими з яких є безпека і конфіденційність даних [14].

Висновки до розділу 2

У цьому розділі було проведено дослідження структури та архітектури мережі VaNet. Структура мережі VaNet: Мережа VaNet має складну структуру, яка складається з транспортних засобів, придорожних блоків (RSU), інфраструктурних вузлів (AP) та інших елементів. Вона може бути організована у вигляді дерева, мережі Mesh або MANET, залежно від вимог і умов розгортання.

Особливості мережі VaNet: Мережа VaNet має свої особливості, включаючи високу мобільність транспортних засобів, обмежені ресурси, високі вимоги до якості обслуговування, потребу в безпековому зв'язку та підтримку реального часу. Ці особливості впливають на вибір архітектури та протоколів в мережі VaNet.

Протоколи маршрутизації в мережах VaNet: Для забезпечення ефективного маршрутизації в мережах VaNet використовуються різні протоколи, такі як маршрутизація на основі позиції, маршрутизація на основі топології та гібридні протоколи. Кожен з цих протоколів має свої переваги та обмеження, і вибір протоколу залежить від вимог мережі та умов розгортання.

Дослідження структури та архітектури мережі VaNet надало нам глибше розуміння цієї типової транспортної мережі. Відомості, отримані з цього дослідження, стануть основою для подальшого розвитку протоколів, алгоритмів та систем у мережі VaNet з метою покращення її ефективності та функціональності.

РОЗДІЛ 3.
КІБЕРБЕЗПЕКА МЕРЕЖ VANET: ЗАГРОЗИ , ВРАЗЛИВОСТІ, АТАКИ

3.1 Питання безпеки та конфіденційності у VaNet

Швидкий розвиток і поширення бездротового зв'язку та інформаційних технологій революціонізують багато аспектів способу життя людини. Конвергенція цих технологій дозволяє надавати широкий спектр послуг і програм як персоналу, так і громадського характеру. Сфера застосування, яка, як очікується, принесе значну користь від цього, — вдосконалена безпека транспортних засобів. Виробники автомобілів почали впроваджувати деякі бездротові інформаційно-комунікаційні технології (ІКТ) у свої автомобілі з програмами, що охоплюють безпеку, ефективність руху, допомогу водієві та інформаційно-розважальні системи [30]. Вони використовують виділений зв’язок малого радіусу дії (DSRC) для доставки цих програм. Мета полягає в тому, щоб мати повністю інтегровані інтелектуальні транспортні системи (ITS), які підвищать загальну безпеку та ефективність транспорту в майбутньому.

Такі мережі, відомі як Vehicle-to-Everything (V2X) мережі, включають в себе комунікацію між транспортними засобами (V2V), транспортними засобами та інфраструктурою (V2I), транспортними засобами та пішоходами (V2P), транспортними засобами та мережею (V2N) та інші комбінації.

Однією з особливостей цих самоорганізованих мереж є їх здатність автоматично адаптуватися до змінюючихся умов. Транспортні засоби та RSU можуть обмінюватися інформацією про дорожні умови, такі як пробки, аварії, обмеження швидкості, а також про дії інших учасників руху. Це дозволяє покращити безпеку на дорозі, оптимізувати рух транспорту та забезпечити більш ефективне використання дорожньої інфраструктури.

Mesh мережі, які використовуються в V2X комунікації, забезпечують багатошляхову комунікацію між різними вузлами мережі. Кожен транспортний засіб або RSU може служити вузлом маршрутизації, передавати повідомлення іншим вузлам і допомагати у встановленні оптимальних шляхів передачі даних.

щоб кожному приймачеві решта всіх вузлів мережі ставилися у відповідність як відправники.

Код, що відповідає за завдання вузлів-отримувачів, виглядає наступним чином:

```
for (uint32_t i = 0; i < m_nSinks; i++){
    Ptr<Socket> sink = SetupRoutingPacketReceive (adhocTxInterfaces.GetAddress (i), c.Get (i));
    AddressValue remoteAddress (InetSocketAddress (adhocTxInterfaces.GetAddress (i), m_port));
    onoff1.SetAttribute ("Remote", remoteAddress);
    ApplicationContainer temp = onoff1.Install (c.Get (i + m_nSinks));
    temp.Start (Seconds (var->GetValue (1.0,2.0)));
    temp.Stop (Seconds (m_TotalSimTime));
}
```

де i – індекс вузла-одержувача, m_nSinks – загальна кількість вузлів-одержувачів.

Потім виконується додавання до коду протоколів, вибраних для аналізу. Для цього достатньо в частину коду, в якій реалізується вибір протоколів додати помічники нових протоколів, які забезпечать можливість подальшої роботи з ними, після цього додати нові відгалуження умов для протоколів та в цих відгалуженнях здійснити додавання нових протоколів до класу помічник, який відповідає за маршрутизацію відповідно з доданими до нього протоколами, а також у змінну відповідну за ім'я протоколу додати назву протоколу, що встановлюється.

Нарешті потрібно встановити бажаний розмір пакета. Для цього в методі, що відповідає за конфігурування параметрів передачі пакетів, у рядку, що встановлює розмір пакетів:

```
Config::SetDefault ("ns3::OnOffApplication::PacketSize",”64”);
```

У рядку зараз встановлено значення частоти, що дорівнює параметру m_rate, який встановлюється як один з аргументів запуску симуляції з командного рядка. У цьому випадку необхідно встановити інтервал відправлення пакетів 0,25 секунди.

Таким чином, підготовка симулятора та сценаріїв для математичного моделювання завершено.

опосередковано можна віднести і до розумної мережі енергопостачання, виходячи із загального становища і спираючись на сукупність всіх вищезазначених і вищезазначених фактів було вирішено запрограмувати деякі пристрої. На рис. 4.21 представлено таблицю умов роботи IoT пристроїв.

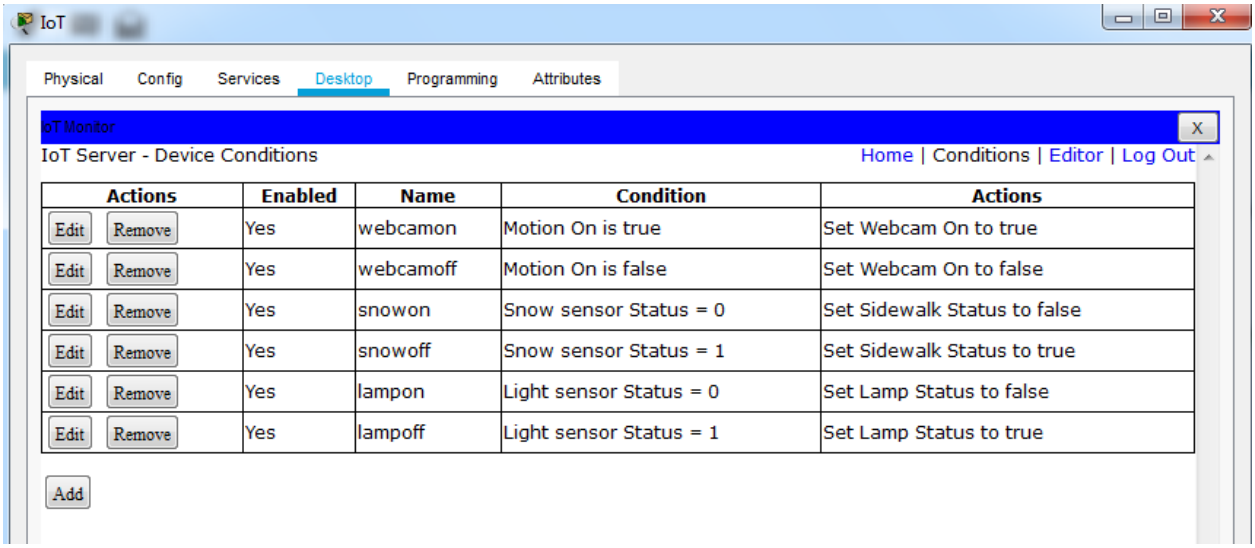

Рисунок 4.21 – Таблиця умов функціонування IoT пристроїв

Отже, даним прикладом було показано розробку та налаштування мережі Smart City, як елементу системи V2I на вирішення завдань організації мережевого взаємодії.

Висновки до розділу 4

У цьому розділі проаналізовано засобів моделювання бездротових сенсорних мереж та розглянуто імітаційне моделювання мережі VANET, який показав, що дані технології швидко розвиваються і існує багато програмних засобів для моделювання бездротових сенсорних мереж. У розділі було обрано систему моделювання NS-3 та показано стартові команди налаштування та створення мережі.

Розглянута прикладна розробка мережі "розумного" міста, що використовує мережу з використанням пристроїв IoT, які є структурними елементами системи V2I (Vehicle-to-Infrastructure). Цей підхід дозволяє створити ефективну систему взаємодії між транспортними засобами та інфраструктурою міста, що сприяє поліпшенню безпеки та ефективності руху.

ВИСНОВКИ

Самоорганізовані транспортні мережі VaNet є бездротовими мережами, які забезпечують спілкування між транспортними засобами та придорожніми блоками. Вони мають характеристики бездротового зв'язку, мобільності, самоорганізації та підтримки реального часу.

Мережі Ad-Hoc, такі як Mesh і MANET, є підтипами самоорганізованих мереж і мають свої властивості та принципи роботи. Мережі Mesh мають гнучку структуру, а MANET є мобільними мережами без потреби в попередній інфраструктурі.

Технології Wi-Fi, зокрема стандарти IEEE 802.11p, є важливими для забезпечення бездротового зв'язку у VaNet. Ці стандарти визначають протоколи та механізми для безпеки, мобільності та якості обслуговування в мережах VaNet.

Структура мережі VaNet: Мережа VaNet має складну структуру, яка складається з транспортних засобів, придорожних блоків (RSU), інфраструктурних вузлів (AP) та інших елементів. Вона може бути організована у вигляді дерева, мережі Mesh або MANET, залежно від вимог і умов розгортання.

Особливості мережі VaNet: Мережа VaNet має свої особливості, включаючи високу мобільність транспортних засобів, обмежені ресурси, високі вимоги до якості обслуговування, потребу в безпековому зв'язку та підтримку реального часу. Ці особливості впливають на вибір архітектури та протоколів в мережі VaNet.

Протоколи маршрутизації в мережах VaNet: Для забезпечення ефективного маршрутизації в мережах VaNet використовуються різні протоколи, такі як маршрутизація на основі позиції, маршрутизація на основі топології та гібридні протоколи. Кожен з цих протоколів має свої переваги та обмеження, і вибір протоколу залежить від вимог мережі та умов розгортання.

Питання безпеки та конфіденційності у VaNet: Мережі VANET стикаються з великими викликами у забезпеченні безпеки та конфіденційності. Вони

вимагають механізмів для захисту від несанкціонованого доступу, аутентифікації, шифрування даних та запобігання зловживанням.

Загрози та виклики безпеці VANET: У мережах VANET існує багато потенційних загроз, таких як атаки на маршрутизацію, фальшиві повідомлення, затримки та втрати даних, фізичні атаки та багато інших. Ці загрози можуть спричинити неправильне функціонування мережі та навіть привести до серйозних наслідків для безпеки учасників дорожнього руху.

Найпоширеніші атаки та їх таксономія: В мережах VANET існують різні типи атак, такі як атаки на маршрутизацію, атаки на аутентифікацію, атаки на конфіденційність, атаки на доступ до ресурсів і фізичні атаки. Класифікація цих атак допомагає визначити їх характеристики та виявити способи захисту від них.

Проаналізовано засобів моделювання бездротових сенсорних мереж та розглянуто імітаційне моделювання мережі VANET, який показав, що дані технології швидко розвиваються і існує багато програмних засобів для моделювання бездротових сенсорних мереж. У розділі було обрано систему моделювання NS-3 та показано стартові команди налаштування та створення мережі.

Показали, що моделювання бездротових сенсорних мереж є важливим інструментом для дослідження та розробки нових технологій та алгоритмів. Використання відповідних засобів моделювання дозволяє ефективно вивчати та оцінювати різні аспекти мереж, а також розробляти та тестувати нові ідеї та рішення.

Розглянута прикладна розробка мережі "розумного" міста, що використовує мережу з використанням припристроїв IoT, які є структурними елементами системи V2I (Vehicle-to-Infrastructure). Цей підхід дозволяє створити ефективну систему взаємодії між транспортними засобами та інфраструктурою міста, що сприяє поліпшенню безпеки та ефективності руху.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Seliem, H.; Shahidi, R.; Ahmed, M.H.; Shehata, M.S. Drone-Based Highway-VANET and DAS Service. IEEE Access 2018, 6, 20125–20137

2. Zhang, D.; Ge, H.; Zhang, T.; Cui, Y.-Y.; Liu, X.; Mao, G. New Multi-Hop Clustering Algorithm for Vehicular Ad Hoc Networks. IEEE Trans. Intell. Transp. Syst. 2018

3. GRIECO, Luigi Alfredo, et al. Ad-hoc, mobile, and wireless networks. In: Proceedings of the 19th international conference on ad-hoc networks and wireless, ADHOC-NOW. 2020. p. 19-21.

4. Li, Xirong, et al. W2vv++ fully deep learning for ad-hoc video search. In: Proceedings of the 27th ACM international conference on multimedia. 2019. p. 1786-1794.

5. Arnous, Reham; EL-Kenawy, E. S. M. T.; Saber, M. A proposed routing protocol for mobile ad hoc networks. Int. J. Comput. Appl, 2019, 975: 8887.

6. Cilfone, Antonio, et al. Wireless mesh networking: An IoT-oriented perspective survey on relevant technologies. Future Internet, 2019, 11.4: 99.

7. Srivastava, Ankita; Prakash, Arun; Tripathi, Rajeev. Location based routing protocols in VANET: Issues and existing solutions. Vehicular Communications, 2020, 23: 100231.

8. Named Data Networking: A Survey on Routing Strategies //Farhan Ahmed Karim, Azana Hafizah Mohd Aman, Rosilah Hassan, (Senior Member, IEEE), Kashif Nisar, (Senior Member, IEEE), Mueen Uddin Режим доступу: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9864583)

9. A Survey of Pr y of Protocol-Le ocol-Level Challenges and Solutions for el Challenges and Solutions for Distributed Energy Resource Cyber-Physical Security Aditya Sundararajan Aniket Chavan Danish Saleem Arif I. Sarwat Режим доступу: https://digitalcommons.fiu.edu/cgi/viewcontent.cgi?article=1065&context=ece_fac

10. AirTies Wireless Networks — Technology. Режим доступу: http://www.airties.com/ technology.html.

42 Strbac, S. A Study of Vehicular Ad-hoc Networks / Stefan Strbac // ENSC 427: Communication networks., 2012, p. 26

43 C. Sommer. A computationally inexpensive empirical model / D. Eckhoff, R. German, and F. Dressler. C. Sommer // IEEE International Conference on Wireless On-Demand Network Systems and Services (WONS), 2011, pp. 84-90

44 Anjali P. Performance Analysis and Comparison of various Radio Propagation models and its impact on Routing Efficiency / Patel Anjali H., Bandana Kumari, Thyagarajan Jayavignesh // National Conference on Science, Engineering and Technology (NCSET)., 2016, pp. 13-16.