ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ

Пояснювальна записка

до магістерської роботи

на тему: **“ Розробка методу забезпечення стійкої роботи сенсорних мереж”**

Виконав: студент 7 курсу, групи
АРЗМ-71
спеціальності
172 Телекомунікації і радіотехніка
(шифр і назва спеціальності)
Копилов А.І.
(прізвище та ініціали)
Керівник
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)

Нормоконтроль_____

Київ - 2021

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

APTEEN	Адаптивний періодичний чутливий до порогових значень енергоефективний протокол сенсорної мережі
BPN	Нейронні мережі зворотного поширення
CDMA	Множинний доступ з кодовим розділенням каналів
DR	Частота виявлення
ELM	Машини екстремального навчання
FN	Хибно негативний
FP	Хибно позитивний
GAF	Географічна адаптивна вірність
GPS	Глобальна система позиціонування
HIDS	Хост-система виявлення вторгнень
IDS	Система виявлення вторгнень
IPS	Система запобігання вторгнень
LEACH	Низькоенергетична адаптивна кластерна ієрархія
LS-SVM	Метод опорних векторів найменших квадратів
MAC	Управління доступом до носія
MCU	Мікроконтролерний блок
NIDS	Мережева система виявлення вторгнень
NSL-KDD	Спеціальний набір даних
RBF	Мережа радіальних базисних функцій
RELM	Правила і машина екстремального навчання
RVFL	Випадкові векторні функціональні посилання
SLFN	Мережі прямого зв’язку з одним прихованим рівнем
SPIN	Протоколи для інформації через переговори
SVM	Метод опорних векторів
TDMA	Множинний доступ з часовим розділенням каналів
TEEN	Чутливий до порогових значень енергоефективний протокол сенсорної мережі
TN	Істино негативний
TNR	Істина негативна норма
TP	Істино позитивний
TPR	Істина позитивна норма
АЦП	Аналого-цифровий перетворювач
БСМ	Бездротова сенсорна мережа

ВСТУП

Актуальність. Актуальність дослідження полягає у тому, що зі стрімким розвитком бездротових сенсорних мереж, що повинні обробляти великі масиви даних, з'явилася необхідність оптимізації традиційної архітектури мережі для забезпечення передачі та обробки цих даних з якомога більшою ефективністю і при цьому забезпечуючи стійку роботу мережі.

Важливою проблемою в БСМ є обмеження енергії. Споживання енергії для передачі даних є вищою, ніж споживання енергії під час будь-якої іншої обробка в БСМ. Споживання енергії є найважливішим фактором для визначення терміну служби сенсорної мережі, оскільки зазвичай сенсорні вузли керуються акумулятором. Іноді оптимізація енергії в сенсорних мережах ускладняється, оскільки вона передбачає не тільки зниження енергоспоживання, але і максимально продовжує термін служби мережі. Скорочення передачі даних зменшило б енергоспоживання мережі, що збільшить термін її служби.

Одним із визначальних факторів які впливають на енергоефективність бездротової сенсорної мережі є безпека. Традиційні заходи захисту інформації не завжди застосовні через обмежені обчислювальні та енергетичні ресурси сенсорних вузлів та мережі в цілому.

Мета й завдання дослідження

Метою роботи є модифікувати архітектуру бездротової сенсорної мережі за рахунок алгоритму машини екстремального навчання для забезпечення стійкої роботи телекомунікаційної мережі.

Для досягнення мети дослідження було поставлено та вирішено такі **основні задачі**:

1. Проаналізувати існуючу архітектуру бездротової сенсорної мережі.
2. Провести аналіз видів атак та їх виявлення у бездротових сенсорних мережах.

3. Провести аналіз алгоритму машини екстремального навчання для обробки даних в бездротових сенсорних мережах.
4. Модифікувати архітектуру бездротової сенсорної мережі для підвищення ефективності передачі та забезпечення стійкої роботи за рахунок використання машини екстремального навчання.
5. Провести імітаційне моделювання бездротової сенсорної мережі на основі модифікованої архітектури, що дозволить оцінити працездатність та ефективність запропонованого рішення.

Об'єкт дослідження: бездротова сенсорна мережа.

Предмет дослідження: Метод забезпечення стійкої роботи сенсорних мереж.

Методи дослідження: основні методи дослідження загальної задачі – це методи системного аналізу а також натурно-імітаційного моделювання. Методи системного аналізу використовуються для агрегування розглянутих окремо сутностей у єдину систему.

Методи натурно-імітаційного моделювання були застосовані при створені робочого макету та при обробці результатів моделювання.

Наукова новизна одержаних результатів

Модифікована архітектура бездротової сенсорної мережі для підвищення ефективності передачі та забезпечення стійкої роботи з використанням алгоритму машини екстремального навчання.

Практичне значення одержаних результатів

Імітаційна модель модифікованої архітектури, що доводить зменшення навантаження на комунікаційну мережу.

РОЗДІЛ 1

ОСОБЛИВОСТІ ПОБУДОВИ ТА ФУНКЦІОНУВАННЯ БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖ

Бездротові сенсорні мережі можуть бути визначені як самоналаштовані бездротові мережі без інфраструктури для моніторингу фізичних або екологічних умов, таких як температура, звук, вібрація, тиск, рух чи забруднювачі, та для спільної передачі своїх даних через мережу на основну локацію або приймач, де можна буде спостерігати за даними та аналізувати їх. Приймач або базова станція діють як інтерфейс між користувачами та мережею.

Бездротові сенсорні мережі складаються з набору датчиків для спостереження за фізичними або екологічними подіями. На даний момент, сенсорні мережі використовуються у таких важливих областях, як військова, медична та цивільний контроль.

Можна отримати необхідну інформацію з мережі, вводячи запити та збираючи результати з приймача. Зазвичай бездротова сенсорна мережа містить сотні тисяч сенсорних вузлів. Сенсорні вузли можуть спілкуватися між собою за допомогою радіосигналів. Бездротовий сенсорний вузол облаштований чутливими та обчислювальними пристроями, радіопередавачами та активними компонентами. Окремі вузли в БСМ обмежені ресурсами: вони мають обмежену швидкість обробки, ємність зберігання та пропускну здатність зв'язку. Після розгортання сенсорних вузлів, вони відповідають за самоорганізацію відповідної мережевої інфраструктури, часто при багато-скачковому багатопотоковому спілкуванні з ними. Потім бортові датчики починають збирати необхідну інформацію. Бездротові сенсорні пристрої також відповідають на запити, надіслані з «контрольного сайту», щоб виконати конкретні вказівки або надати зразки. Режим роботи сенсорних вузлів може бути безперервний або керований подіями. Для отримання інформації про місцеположення можна використовувати глобальну систему позиціонування (GPS) та локальні

алгоритми позиціонування. Бездротові сенсорні пристрої можуть бути обладнані виконавчими механізмами для "дії" за певних умов [1].

Оскільки це бездротовий носій, розміщений у віддалених місцях та обмежений ресурсом, сенсорні мережі дуже вразливі до атак. Атака завдає значних пошкоджень сенсорним мережам. Щоб уникнути цих проблем, на базовій станції впроваджена система виявлення вторгнень (IDS) для фільтрації будь-яких аномальних пакетів.

1.1 Аналіз концепції бездротових сенсорних мереж

БСМ дозволяють створювати нові програми та вимагають нетрадиційних парадигм для розробки протоколу через декілька обмежень. За рахунок низької вимоги складності пристрою разом із низьким енергоспоживанням (тобто тривалий термін служби мережі) повинен бути встановлений належний баланс між можливостями зв’язку та обробкою сигналів / даних. Це мотивує величезні зусилля в науково-дослідній діяльності, стандартизації та промислових інвестиціях у цій галузі за останнє десятиліття [2]. В даний час більшість досліджень щодо БСМ зосереджені на розробці енергоефективних та обчислювально-ефективних алгоритмів та протоколів, а область застосування обмежена простими програмами моніторингу та звітності, орієнтованими на дані [3].

Автори [4] пропонують алгоритм переходу кабельного режиму, який визначає мінімальну кількість активних датчиків для підтримки K-покриття місцевості, а також K-підключення мережі. Зокрема, він виділяє періоди бездіяльності для кабельних датчиків, не впливаючи на вимоги покриття та підключення до мережі, грунтуючись лише на локальній інформації. У [5] запропонована структура мережі збору даних враховуючи затримки для бездротових сенсорних мереж. Метою запропонованої структури мережі - мінімізувати затримки в процесах збору даних бездротових сенсорних мереж, що продовжує термін служби мережі. У роботі [6] автори розглядають ретрансляційні вузли для зменшення геометричних недоліків мережі та

використовують алгоритми, засновані на оптимізації частинок, щоб знайти оптимальне місцерозташування приймача відносно цих ретрансляційних вузлів для подолання проблеми терміну служби. Енергоефективна комунікація також була розглянута в [7], в цій роботі автори пропонують геометричне рішення для визначення оптимального розміщення приймача для максимізації терміну служби мережі.

У більшості випадків в дослідженнях бездротових сенсорних мереж розглядались однорідні сенсорні вузли. Але у даний час дослідники зосереджуються на гетерогенних сенсорних мережах, де сенсорні вузли відрізняються один від одного з точки зору їх енергії. У роботі [8] автори розглядають проблему розгортання ретрансляційних вузлів для забезпечення відмовостійкості з більш високою зв'язністю мереж в гетерогенних бездротових сенсорних мережах, де сенсорні вузли мають різні радіуси передачі. Нові мережеві архітектури з неоднорідними пристроями та нещодавній прогрес у цій технології усувають поточні обмеження та значно розширюють спектр можливих застосувань для БСМ, і все це дуже швидко змінюється.

1.2 Структура бездротового сенсорного вузла

Сенсорний вузол складається з чотирьох основних компонентів, таких як сенсорний блок, блок обробки, приймач-передавач і блок живлення, показаний на рис. 1.1. В залежності від застосування, він також має додаткові компоненти, такі як система визначення місцяположення, генератор живлення та мобілізатор.

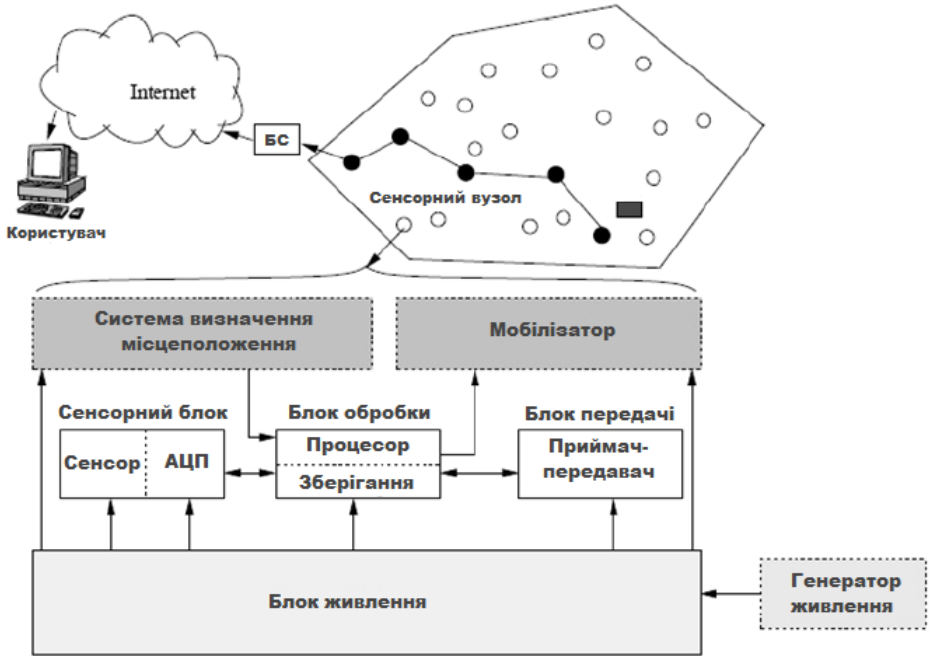

Рисунок 1.1 Компоненти сенсорного вузла

Сенсорні блоки зазвичай складаються з двох субодиниць: датчиків та аналого-цифрових перетворювачів (АЦП) [9]. Аналогові сигнали, що створюються датчиками, за допомогою АЦП перетворюються в цифрові сигнали, а потім надходять в блок обробки. Блок обробки, як правило, пов'язаний з невеликим блоком зберігання, і він може керувати процедурами, завдяки яким сенсорний вузол співпрацює з іншими вузлами для виконання завдань виявлення. Приймач-передавач з'єднує вузол з мережею. Один з найважливіших компонентів сенсорного вузла - це блок живлення. Блоки живлення можуть підтримуватися енергозберігаючим блоком, наприклад сонячними елементами. Інші субодиниці вузла залежать від програми.

Модульна конструкція бездротового чутливого вузла забезпечує гнучку та універсальну платформу для задоволення потреб широкого спектру застосувань. Наприклад, залежно від датчиків, які будуть розгорнуті, блок формування сигналу можна перепрограмувати або замінити. Це дозволяє використовувати широкий спектр різних датчиків з бездротовим сенсорним вузлом. Аналогічно, радіозв'язок може бути замінений, у відповідності до

вимог бездротового діапазону для певних додатків та необхідності двонаправленої комунікації.

Використовуючи флеш-пам'ять, віддалені вузли отримують дані по команді з базової станції або за подією, що приймається одним або декількома входами до вузла. Більше того, вбудовану прошивку можна модернізувати через бездротову мережу на місці. Мікропроцесор має ряд функцій, включаючи:

- керування збором даних з датчиків
- виконання функцій управління потужністю
- взаємодія даних сенсорів з фізичним рівнем радіозв'язку
- управління протоколом радіомережі

Ключовим аспектом будь-якого бездротового чутливого вузла є мінімізація споживаної системою енергії. Зазвичай підсистема радіозв'язку вимагає найбільшої кількості енергії. Тому дані надсилаються по радіомережі лише тоді, коли це необхідно. Алгоритм повинен бути завантажений у вузол, щоб визначити, коли надсилати дані на основі виявленної події. Крім того, важливо мінімізувати енергію, яка споживається самим датчиком. Тому, обладнання повинно бути розроблене так, щоб мікропроцесор міг розсудливо керувати живленням радіомодуля, датчика та датчика формування сигналу [9].

1.3 Структура зв'язку бездротової сенсорної мережі

Сенсорні вузли, як правило, розкидані в сенсорному полі, як показано на рис. 1.3. Кожен з цих розсіяних сенсорних вузлів має можливість збирати дані та направляти дані назад до приймача та кінцевих користувачів. Дані передаються назад кінцевому користувачеві за допомогою багато-скачкової архітектури без інфраструктури, через приймач, як показано на рис. 1.2. Приймач може спілкуватися з вузлом диспетчера завдань через Інтернет або Супутник.

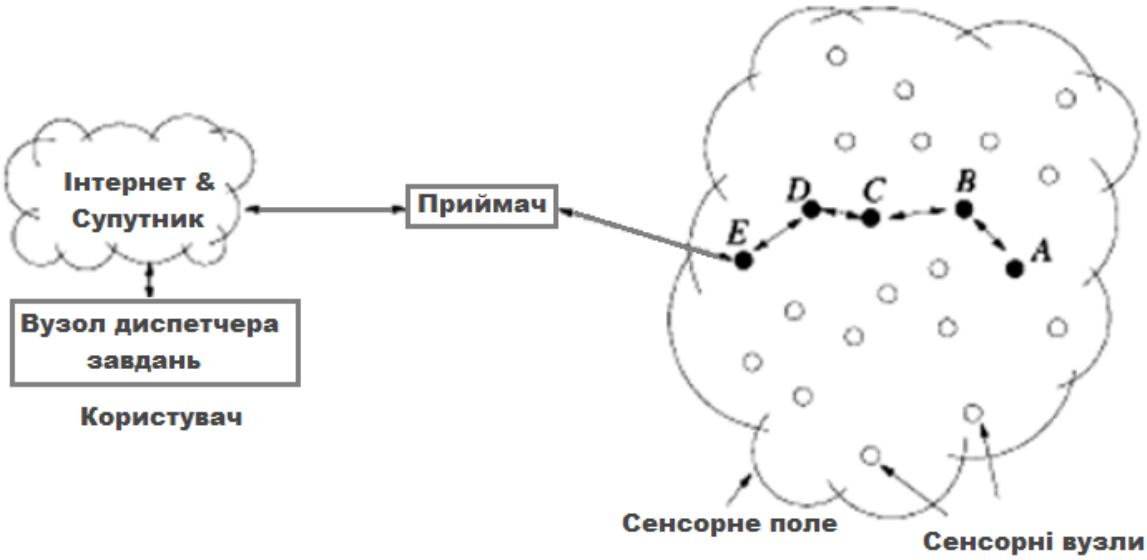

Рисунок 1.2 Типічна бездротова сенсорна мережа

Стек протоколів, який використовується приймачем та сенсорними вузлами, наведений на рис. 1.3. Цей стек протоколів поєднує в собі інформацію про потужність та маршрутизацію, інтегрує дані з мережевими протоколами і ефективно передає енергію за допомогою бездротового середовища.

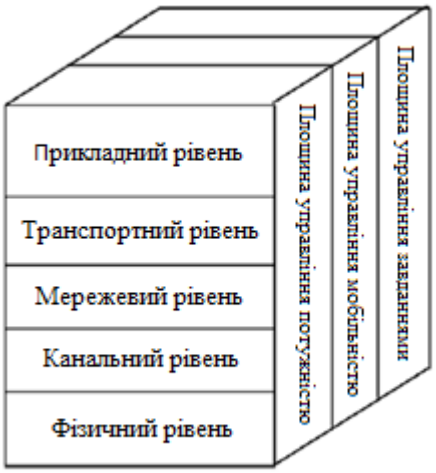

Рисунок 1.3 Стек протоколів бездротової сенсорної мережі

Стек протоколів складається з прикладного рівня, транспортного рівня, мережевого рівня, канального рівня, фізичного рівня, площини управління потужністю, площини управління мобільністю та площини управління

завданнями [9]. На прикладному рівні можуть бути побудовані та використані різні типи прикладного програмного забезпечення залежно від завдань розпізнавання. Цей рівень робить апаратне та програмне забезпечення найнижчого рівня прозорим для кінцевого споживача. Транспортний рівень допомагає підтримувати потік даних, якщо цього вимагає додаток сенсорних мереж. Мережевий рівень дбає про маршрутизацію даних, що надаються транспортним рівнем, певними багато-скачковими протоколами бездротової маршрутизації між вузлами датчика та приймача. Канальний рівень передачі даних відповідає за мультиплексування потоків даних, виявлення кадрів, управління доступом до носія (MAC) та контроль помилок. Оскільки в середовищі шумно і сенсорні вузли можуть бути мобільними, протокол MAC повинен враховувати енергоспоживання і мати можливість мінімізувати конфлікти з трансляцією сусідів. Фізичний рівень відповідає потребам простим, але надійним методам модуляції, вибору частоти, методів шифрування даних, передачі та прийому.

Крім того, площини управління потужністю, мобільністю та завданнями контролюють потужність, рух та розподіл задач між сенсорними вузлами. Ці площини допомагають вузлам датчиків координувати завдання вимірювання і знижувати загальне споживання енергії.

1.4 Проблеми енергоспоживання в бездротовій сенсорній мережі

Споживання енергії є найважливішим фактором для визначення терміну служби сенсорної мережі, оскільки зазвичай сенсорні вузли керуються акумулятором. Іноді оптимізація енергії в сенсорних мережах ускладняється, оскільки вона передбачає не тільки зниження енергоспоживання, але і максимально продовжує термін служби мережі. Оптимізація може бути здійснена, маючи енергетичну обізнаність в усіх аспектах проектування та експлуатації. Це забезпечує включення енергетичної обізнаності також у групи комунікаційних сенсорних вузлів та всієї мережі, а не лише в окремих вузлах [10].

Сенсорний вузол зазвичай складається з чотирьох підсистем [10]:

- обчислювальна підсистема: вона складається з мікропроцесора (мікроконтролерного блоку, MCU), який відповідає за управління датчиками та впровадження протоколів зв'язку. MCU зазвичай працюють в різних режимах для управління енергією. Оскільки ці режими роботи передбачають споживання енергії, слід враховувати рівні споживання енергії в різних режимах, враховуючи термін роботи акумулятора кожного вузла.
- підсистема зв'язку: вона складається з радіоприймача короткого діапазону, який спілкується із сусідніми вузлами та зовнішнім світом. Радіоприймачі можуть працювати в різних режимах. Важливо повністю вимкнути радіоприймач, а не переводити його в режим очікування, коли він не передає і не отримує дані для економії енергії.
- підсистема зчитування: вона складається з групи датчиків і виконуючих механізмів і зв'язує вузол із зовнішнім світом. Споживання енергії можна зменшити, використовуючи компоненти з низькою потужністю та заощаджуючи електроенергію за рахунок продуктивності, яка не потрібна.
- підсистема електроживлення: вона складається з акумулятора, який подає живлення у вузол. Слід зазначити, що кількість енергії, яка береться від акумулятора, перевіряється, тому що якщо великий струм витягується з акумулятора протягом тривалого часу, акумулятор загине швидше, навіть якщо б він міг би працювати довше. Зазвичай, номінальна потужність струму акумулятора, що використовується для сенсорного вузла, менше мінімального енергоспоживання. Термін служби акумулятора можна збільшити шляхом різкого зменшення струму або навіть частого його вимикання.

Термін служби сенсорної мережі може бути значно збільшений, якщо операційна система, прикладний рівень та мережеві протоколи розроблені з урахуванням енергозберігання. Ці протоколи та алгоритми повинні бути обізнаними з обладнанням і мати можливість використовувати особливості

мікропроцесорів та приймач-передавчів, щоб мінімізувати споживання енергії сенсорного вузла. Це може підштовхнути до індивідуального рішення для різних типів конструкцій сенсорних вузлів. Різні типи розгорнутих сенсорних вузлів також призводять до різних типів сенсорних мереж. Це також може призвести до різних типів алгоритмів спільної роботи на бездротових сенсорних мережах.

1.5 Протоколи та алгоритми бездротової сенсорної мережі

У бездротових сенсорних мережах головне завдання сенсорного вузла - це виявлення даних і передача їх на базову станцію в багато-скачковому середовищі, для якого необхідний шлях маршрутизації. Для обчислення шляху маршрутизації від вихідного вузла до базової станції існує величезна кількість запропонованих протоколів маршрутизації [3]. Конструкція протоколів маршрутизації для бездротових сенсорних мереж повинна враховувати обмеження потужності та ресурсів мережевих вузлів, змінювана в часі якість бездротового каналу, можливість втрати та затримки пакетів. Для вирішення цих вимог до проектування було запропоновано кілька стратегій маршрутизації для БСМ [3].

Перший клас протоколів маршрутизації приймає плоску мережеву архітектуру, в якій всі вузли вважаються рівноправними. Архітектура плоскої мережі має ряд переваг, включаючи мінімальні накладні витрати на підтримку інфраструктури та можливість виявлення декількох маршрутів між вузлами зв'язку для забезпечення відмовостійкості.

Другий клас протоколів маршрутизації накладає структуру в мережу для досягнення енергоефективності, стабільності та масштабованості. У цьому класі протоколів мережеві вузли організовані в кластери, в яких, наприклад, вузол з більшою залишковою енергією бере на себе роль голови кластера. Голова кластера відповідає за координацію діяльності всередині кластеру та передачу інформації між кластерами. Кластеризація може потенційно зменшити споживання енергії та продовжити термін експлуатації мережі.

Третій клас протоколів маршрутизації використовує підхід, орієнтований на дані, для поширення інтересів у мережі. У підході використовується іменування на основі атрибутів, при якому вихідний вузол робить запит на атрибут явища, а не окремий сенсорний вузол. Поширення інтересів досягається шляхом призначення завдань сенсорним вузлам і висловленням запитів відносно конкретних атрибутів. Для передачі інтересів до сенсорних вузлів можуть використовуватися різні стратегії, включаючи трансляцію, багатоадресову передачу на основі атрибутів.

Четвертий клас протоколів маршрутизації використовує місцеположення для адресації сенсорного вузла. Маршрутизація на основі місцеположення корисна в додатках, коли положення вузла в межах географічного покриття мережі відповідає запиту, виданому вихідним вузлом. Такий запит може вказувати конкретну область, де може статися певне явище, або близькість до певної точки в мережевому середовищі.

Далі буде розглянуто деякі з основних протоколів маршрутизації та алгоритми, що стосуються проблеми енергозбереження.

1. Затоплення (Flooding): Затоплення - це розповсюджений метод, який часто застосовується для виявлення шляхів та розповсюдження інформації в дротових та бездротових спеціальних мережах, про які йшлося в [9]. Стратегія маршрутизації затоплення проста і не залежить від високовартісного обслуговування топології мережі та складних алгоритмів виявлення маршруту. Затоплення використовує реактивний підхід, згідно з яким кожен вузол, який отримує пакет даних або управління, відправляє пакет усім своїм сусідам. Після передачі пакет слідує за всіма можливими шляхами. Якщо мережа не відключена, пакет врешті-решт досягне свого пункту призначення. Крім того, при зміні топології мережі, переданий пакет слідує новими маршрутами. Рис. 1.4 ілюструє концепцію затоплення в мережі передачі даних. Як показано на рисунку, затоплення у найпростішому вигляді може спричинити нескінченне копіювання пакетів мережевими вузлами.

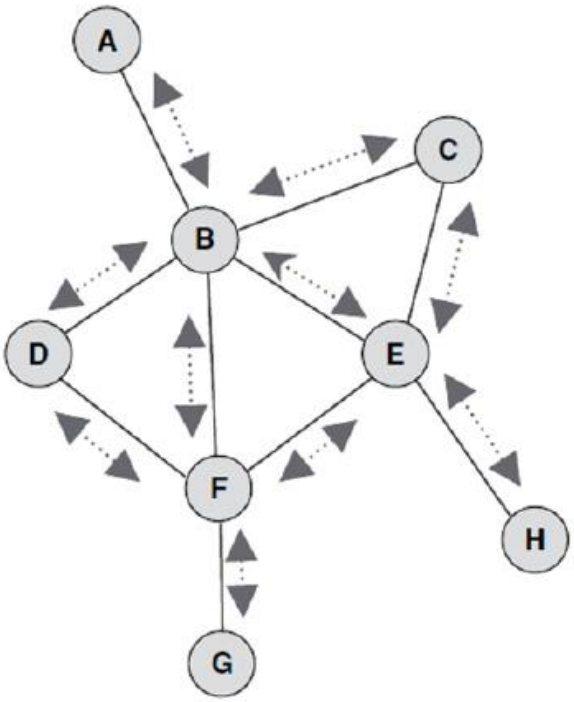

Рисунок 1.4 Затоплення в мережі передачі даних

2. Плітки (Gossiping):

Для усунення недоліків затоплення було запропоновано похідний підхід, іменований плітками [9]. Подібно до затоплення, плітки використовують просте правило переадресації і не вимагають високовартісного обслуговування топології або складних алгоритмів виявлення маршруту. На відміну від затоплення, коли пакет даних транслюється всім сусідам, плітки вимагають, щоб кожен вузол надсилав вхідний пакет випадково вибраному сусідові. Отримавши пакет, сусід, вибраний випадковим чином, вибирає одного з своїх власних сусідів і пересилає пакет обраному сусідові. Цей процес триває ітераційно, поки пакет не досягне свого цільового призначення або не буде перевищено максимальну кількість стрибків.

3. Протоколи для інформації за допомогою переговори (SPIN):

Сенсорні протоколи інформації за допомогою переговорів (SPIN) - це засноване на даних сімейство протоколів поширення інформації для БСМ [11]. Основна мета цих протоколів - ефективно поширювати спостереження, зібрані окремими сенсорними вузлами, на всі сенсорні вузли в мережі. Прості протоколи, такі як затоплення та плітки, зазвичай пропонуються для поширення інформації у БСМ. Затоплення вимагає, щоб кожен вузол надсилав копію пакету даних усім своїм сусідам, поки інформація не досягне всіх вузлів мережі. З іншого боку, плітки використовують рандомізацію для зменшення кількості повторюваних пакетів і вимагають лише, щоб вузол, що приймає пакет даних, пересилав його до випадково вибраного сусіда.

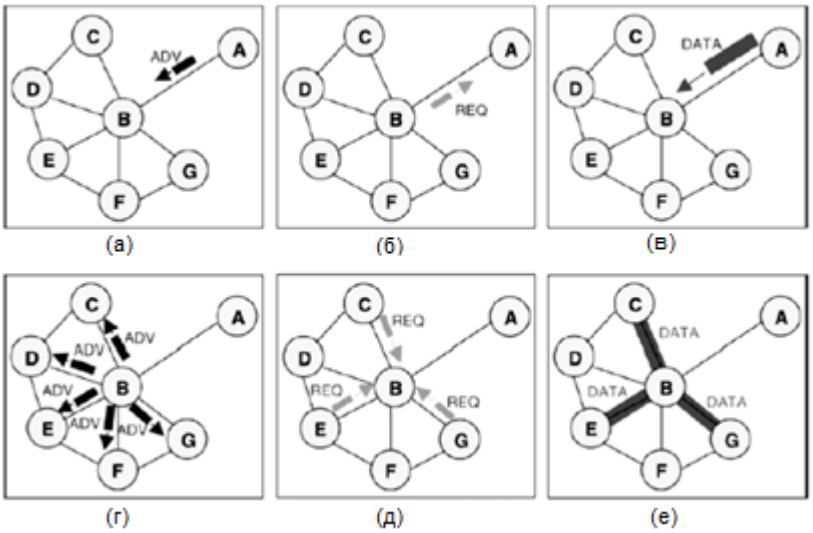

Рисунок 1.5 Основні операціїї протоколу SPIN

4. Низькоенергетична адаптивна кластерна ієрархія (LEACH)

Низькоенергетична адаптивна кластерна ієрархія (LEACH)- алгоритм маршрутизації, призначений для збору та доставки даних до приймача даних, як правило, до базової станції [12].

Основними цілями LEACH є:

- Подовження терміну служби мережі
- Зменшення споживання енергії кожним сенсорним вузлом мережі

- Використання агрегації даних для зменшення кількості комунікаційних повідомлень

Для досягнення цих цілей LEACH застосовує ієрархічний підхід до організації мережі в набір кластерів. Кожен кластер керується вибраною головою кластера. Голова кластера бере на себе відповідальність за виконання декількох завдань. Перше завдання складається з періодичного збору даних від членів кластеру. Після збору даних, голова кластера об'єднує їх, намагаючись усунути надмірність корельованих значень. Другим головним завданням голови кластера є передача агрегованих даних безпосередньо на базову станцію за один скачок. Третє головне завдання голови кластера - створити розклад на основі TDMA, згідно з яким кожному вузлу кластера призначається часовий проміжок, який він може використовувати для передачі. Голова кластера оголошує розклад своїм членам кластеру через трансляцію. Щоб знизити ймовірність зіткнень між датчиками всередині кластера та поза ним, вузли LEACH використовують для зв'язку схему множинного доступу на основі кодового розподілу.

Основні операції LEACH організовані у два окремих етапи. Перший етап, етап налаштування, складається з двох кроків, вибору голови кластера та формування кластера. Другий етап, стаціонарний етап, зосереджений на зборі, агрегації даних та доставці даних на базову станцію. Тривалість установки вважається порівняно коротшою, ніж етап стаціонарного стану, щоб мінімізувати накладні витрати протоколу.

На початку етапу налаштування починається крок вибору голови кластера. Щоб вирішити, чи має вузол стати головою кластера чи ні, порогове значення T(s), розглянуто в [12], полягає в наступному:

$$T(s) = \begin{cases} \frac{p_{opt}}{1-p_{opt}.\left(r.mod.\frac{1}{p_{opt}}\right)}, if s \in G' \\ 0, \text{інакше} \end{cases} \quad (1.1)$$

де r – номер поточного раунду, а G - сукупність вузлів, які не стали головою кластера протягом останніх $1/p_{opt}$ раундів. На початку кожного раунду кожен вузол, який належить до набору G, вибирає випадкове число 0 або 1. Якщо випадкове число менше порогового значення T(s), то вузол стає головою кластера в поточному раунді.

5. Чутливі до порогових значень енергоефективні протоколи (TEEN та APTEEN):

Два протоколи ієрархічної маршрутизації під назвою TEEN (Чутливий до порогових значень енергоефективний протокол сенсорної мережі) та APTEEN (Адаптивний періодичний чутливий до порогових значень енергоефективний протокол сенсорної мережі) запропоновані в [13]. Ці протоколи були запропоновані для критично важливих по часу додатків. У TEEN сенсорні вузли розпізнають носій безперервно, але передача даних відбувається рідше. Датчик голови кластера надсилає своїм членам жорсткий поріг, який є пороговим значенням виявленого атрибута та м'який поріг, який представляє собою невелику зміну у значенні виявленного атрибута, що ініціює вузол для вімкнення його передавача і передачі.

Таким чином, жорсткий поріг намагається зменшити кількість передач, дозволяючи вузлам передавати лише тоді, коли виявлений атрибут знаходиться в зацікавленому діапазоні. М'який поріг додатково зменшує кількість передач, які могли б статися в іншому випадку, коли виявлений атрибут незначний або взагалі не змінюється. Менше значення м'якого порогу дає більш точну картину мережі за рахунок збільшення енергоспоживання. Таким чином, користувач може контролювати компроміс між енергоефективністю та точністю даних. Коли необхідно змінити голову кластера, передаються нові значення для вищезазначених параметрів. Основний недолік цієї схеми полягає в тому, що, якщо порогові значення не отримані, вузли ніколи не будуть обмінюватись даними, і користувач взагалі не отримає жодних даних з мережі.

6. Енергоефективний збір в сенсорних інформаційних системах (PEGASIS):

Енергоефективний збір в сенсорних інформаційних системах (PEGASIS) [14] та його розширення, ієрархічний PEGASIS, є сімейством протоколів маршрутизації та збору інформації для БСМ. Основні цілі PEGASIS - подвійні. По-перше, протокол спрямований на продовження терміну експлуатації мережі шляхом досягнення високого рівня енергоефективності та рівномірного енергоспоживання у всіх вузлах мережі. По-друге, протокол прагне зменшити затримку, яка виникає на шляху до приймача.

Модель мережі, розглянута PEGASIS, передбачає однорідний набір вузлів, розгорнутих в географічій області. Передбачається, що вузли мають загальні знання про положення інших датчиків. Крім того, вони мають можливість контролювати свою силу для покриття довільних діапазонів. Вузли також можуть бути обладнані радіоприйомопередавачами з підтримкою CDMA. Відповідальність вузлів полягає в зборі та доставці даних до приймача, як правило, до бездротової базової станції. Мета - розробити структуру маршрутизації та схему агрегації, щоб зменшити енергоспоживання та доставити агреговані дані до базової станції з мінімальною затримкою, в той же час балансуючи споживання енергії між сенсорними вузлами. На відміну від інших протоколів, які покладаються на деревовидній структурі або ієрархічної організації мережі на основі кластерів для збору та розповсюдження даних, PEGASIS використовує ланцюгову структуру.

7. Направлена дифузія:

Направлена дифузія [14] - орієнтований на дані протокол маршрутизації для збору та розповсюдження інформації у БСМ. Основна мета протоколу - досягти значної економії енергії з метою продовження терміну експлуатації мережі. Для досягнення цієї мети спрямована дифузія підтримує взаємодію між вузлами з точки зору обміну повідомленнями, локалізованого в межах обмеженої мережевої близькості. Використовуючи локалізовану взаємодію,

пряма дифузія все ще може реалізувати надійну доставку з декількома шляхами та адаптуватися до мінімального набору мережевих шляхів. Ця унікальна особливість протоколу в поєднанні зі здатністю вузлів агрегувати відповіді на запити призводить до значної економії енергії.

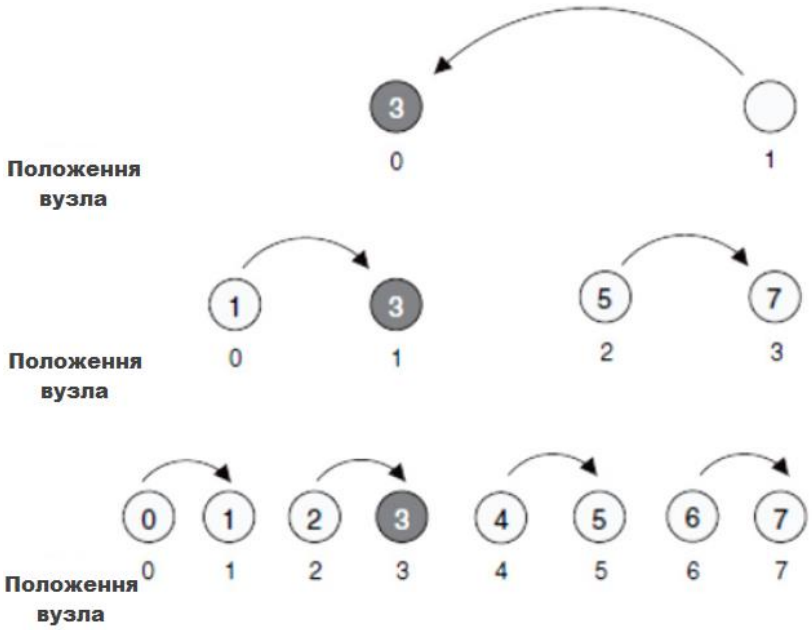

Рисунок 1.6 Схема збору та агрегації даних на основі ланцюга

Основними елементами направлена дифузії є інтереси, повідомлення даних, градієнти та підкріплення. Направлена дифузія використовує інформаційну модель публікації та підписки, в якій запитуючий виявляє інтерес, використовуючи пари атрибут-значення. Інтерес можна розглядати як запит або допит, який визначає, чого хоче запитуючий.

8. Географічна адаптивна вірність (GAF):

GAF [15]– енергозберігаючий алгоритм маршрутизації на основі визначення місцерозташування, розроблений головним чином для мобільних спеціальних мереж, але може застосовуватися і для сенсорних мереж. Область мережі спочатку поділяється на нерухомі зони і утворює віртуальну сітку. Всередині кожної зони вузли взаємодіють один з одним, граючи різні ролі. Наприклад, вузли виберуть один сенсорний вузол, щоб не спати протягом певного періоду часу, а потім вони перейдуть до сплячого режиму.

Цей вузол відповідає за моніторинг та передачу даних в базову станцію від імені вузлів у зоні. Отже, GAF заощаджує енергію, вимикаючи непотрібні вузли в мережі, не впливаючи на рівень точності маршрутизації.

Висновки до розділу

Проведений аналіз концепції бездротових сенсорних мереж. В даний час дослідники зосереджуються на гетерогенних сенсорних мережах, де сенсорні вузли відрізняються один від одного з точки зору їх енергії. Нові мережеві архітектури з неоднорідними пристроями та нещодавній прогрес у цій технології усувають поточні обмеження та значно розширюють спектр можливих застосувань для БСМ, і все це дуже швидко змінюється.

Проаналізовано структуру бездротового сенсорного вузла та виділено основні його компоненти, такі як сенсорний блок, блок обробки, приймач-передавач і блок живлення. Модульна конструкція бездротового чутливого вузла забезпечує гнучку та універсальну платформу для задоволення потреб широкого спектру застосувань. Ключовим аспектом будь-якого бездротового чутливого вузла є мінімізація споживаної системою енергії.

Визначено структуру зв'язку бездротової сенсорної мережі. Сенсорні вузли, як правило, розкидані в сенсорному полі. Кожен з цих розсіяних сенсорних вузлів має можливість збирати дані та направляти дані назад до приймача та кінцевих користувачів. Стек протоколів, який використовується приймачем та сенсорними вузлами, поєднує в собі інформацію про потужність та маршрутизацію, інтегрує дані з мережевими протоколами і ефективно передає енергію за допомогою бездротового середовища. Стек протоколів складається з прикладного рівня, транспортного рівня, мережевого рівня, канального рівня, фізичного рівня, площини управління потужністю, площини управління мобільністю та площини управління завданнями.

Проведений аналіз проблеми енергоспоживання в бездротовій сенсорній мережі. Споживання енергії є найважливішим фактором для визначення терміну служби сенсорної мережі, оскільки зазвичай сенсорні вузли керуються акумулятором. Термін служби сенсорної мережі може бути значно збільшений, якщо операційна система, прикладний рівень та мережеві протоколи розроблені з урахуванням енергозберігання.

Проведений аналіз основних протоколів маршрутизації та алгоритмів, що стосуються проблеми енергозбереження. Конструкція протоколів маршрутизації для бездротових сенсорних мереж повинна враховувати обмеження потужності та ресурсів мережевих вузлів, змінювана в часі якість бездротового каналу, можливість втрати та затримки пакетів. Було розглянуто деякі з основних протоколів маршрутизації та алгоритми, що стосуються проблеми енергозбереження: Затоплення (Flooding), Плітки (Gossiping), Протоколи для інформації за допомогою переговори (SPIN), Низькоенергетична адаптивна кластерна ієрархія (LEACH), Чутливі до порогових значень енергоефективні протоколи (TEEN та APTEEN), Енергоефективний збір в сенсорних інформаційних системах (PEGASIS), Направлена дифузія, Географічна адаптивна вірність (GAF).

РОЗДІЛ 2

ПРОБЛЕМИ БЕЗПЕКИ В БЕЗДРОТОВІЙ СЕНСОРНІЙ МЕРЕЖІ

Проблеми безпеки в сенсорних мережах залежать від необхідності знати, що необхідно захистити. У роботі [16] автори визначили чотири цілі безпеки в сенсорних мережах: конфіденційність, цілісність, аутентифікація та доступність. Конфіденційність - це можливість приховувати повідомлення від пасивного зловмисника, коли повідомлення, передане в сенсорних мережах, залишається конфіденційним. Цілісність означає можливість підтвердити, що повідомлення не було підроблено чи змінено під час його перебування в мережі. Аутентифікація - необхідність знати, чи є повідомлення від вузла, на який він стверджує, визначаючи тим самим надійність походження повідомлення. Доступність - це можливість визначити, чи має вузол можливість використовувати ресурси та чи доступна мережа для передачі повідомлень. Свіжість означає, що одержувач отримує нещодавні та нові дані та гарантує, що жоден супротивник не зможе відтворити старі дані. Ця вимога особливо важлива, коли вузли БСМ використовують спільні ключі для обміну повідомленнями, де потенційний зловмисник може почати атаку відтворення за допомогою старого ключа, оскільки новий ключ оновлюється та розповсюджується на всі вузли БСМ [17].

2.1 Види атак та їх вплив на бездротову сенсорну мережу

У БСМ загрози безпеці сильніше відрізняються від дротових та бездротових мереж. Ці відмінності обумовлені типовими властивостями БСМ. Енергія є важливим обмеженням для БСМ, і крім трьох компонентів безпеки (конфіденційність, цілісність та доступність), є новий базовий аспект - енергія. Далі коротко пояснено ці чотири основні аспекти безпеки БСМ.

- Конфіденційність: у парадигмі кібербезпеки конфіденційність є найвідомішим компонентом, який вартий уваги. Користувачі хочуть

надсилати дані без зловмисників, які виводять вміст. У бездротовій мережевій комунікації легко прослухати дані, що передаються по мережі. Для забезпечення конфіденційності золотим твердженням є "інформація має цінність", і тому користувачі хочуть захистити інформацію від її розкриття небажаним та несанкціонованим сторонам. Для забезпечення конфіденційності, мережа повинна шифрувати дані. Це шифрування може обслуговуватися симетричними та асиметричними методами шифрування. Асиметричне шифрування є більш потужним, ніж симетричне шифрування через свій підхід із приватним ключем, але асиметричне шифрування не є економічно ефективним для енергії. Якщо користувачі БСМ використовують симетричне шифрування, вони повинні бути впевнені в тому, що зберігають свій ключ. Щоб забезпечити цю впевненість, корисний та надійний IDS може попередити користувача про мережеву безпеку або встановити безпечну систему управління ключами в системі БСМ [18].

- Цілісність:

Цілісність захищає дані від небажаних та неавторизованих сторін. Якщо вірна лише інформація, користувачі можуть використовувати її як значення. Бездротові сенсорні мережі відстежують навколишнє середовище, і вони працюють, оцінюючи ці дані, отримані з навколишнього середовища. Щоб забезпечити роботу належним чином, користувачі повинні бути впевнені в цілісності даних. У дротових та неенергетичних бездротових мережах користувачі можуть забезпечити цілісність за допомогою цифрових підписів (хешірувати отримані дані та порівнювати їх з хешами вихідних даних), але такий підхід не підходить для БСМ, оскільки він може спричинити додаткові байти для даних, які передається з будь-якого датчика на інший. Другий негативний вплив підпису полягає в тому, що він потребує додаткових обчислювальних ресурсів. У системах БСМ забезпечення цілісності потребує додаткових обчислювальних ресурсів і створює додаткові байти для даних, що передаються, щоб успішний та енергозберігаючий IDS-архітектор міг забезпечити важливий механізм цілісності.

- Доступність:

Якщо спостерігати за різноманітністю атак, можна легко побачити, що деякі атаки не спрямовані на дані, що передаються по мережі. Є кілька атак, націлених на те, щоб зробити мережу непрацездатною. Інформація має цінність, звичайно, якщо вона є "правдою" (цілісність) і користувач отримує доступ до неї в "справжній час" (доступність). Зловмисники можуть пошкодити доступність для БСМ, надіславши неправдиву інформацію про маршрутизацію, якої не існує. Атака затоплення, атаки на відмову в обсуговувані, атака заклинювання, атаки червоточини - це приклади деяких атак, які орієнтовані на доступність.

- Енергія:

БСМ має енергетичні обмеження, і це впливає на всі плани безпеки, створені для нього. Датчики БСМ мають обмежені обчислювальні ресурси і обмежену енергію. Моніторинг навколишнього середовища БСМ і термін служби датчиків дуже важливі, тому мають слугувати більше часу, а користувачі БСМ уникають скорочення терміну служби акумулятора датчика. Цей енергетичний підхід розглядається як додатковий елемент до компонентів управління кібербезпекою (конфіденційність, цілісність та доступність). При створенні IDS-архітектора для БСМ, необхідно враховувати обмеження енергії.

Окрім класичного підходу до мережевого захисту, безпека БСМ має різні властивості. Ці різні властивості викликають різні методи управління безпекою, різні типи атак та різні контрзаходи. Чотири основні компоненти безпеки БСМ (конфіденційність, цілісність, доступність та енергія) описані вище. Далі описано кібератаки, які відбуваються в бездротових сенсорних мережах.

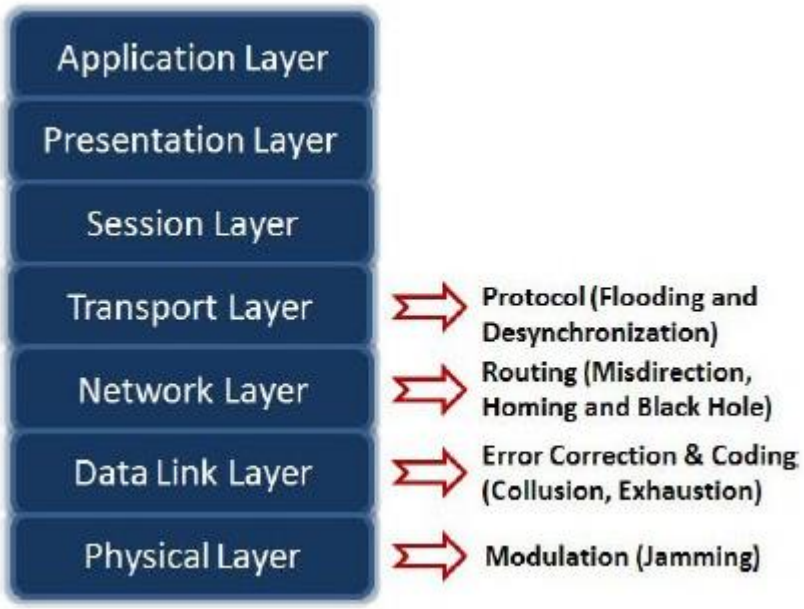

Рисунок 2.1 Типи DoS атак на рівнях БСМ

1. Атаки на відмову в обслуговуванні (DoS)

Основна мета DoS атак - спроба зробити онлайн-сервіс (мережеві ресурси) недоступним, перевантаживши його. Через особливості БСМ, DoS-атаки можуть бути різними. Зловмисники формують вторгнення відповідно до різних особливостей БСМ. Зловмисники хочуть використати слабкі місця БСМ, такі як обмежена пам'ять та обмежені обчислення. У літературі DoS атаки класифікуються на три типи [19]:

- Експлуатація ресурсів, роблячи обмежені ресурси непридатними.
- Конфігурація будь-якої БСМ повинна залишатися в таємниці і повинна бути захищена від змін, зроблених зловмисниками. Тому що ця конфігурація може зазнати вторгнення.
- Фізичне знищення сенсорних пристроїв є дуже небезпечною загрозою для БСМ. Датчики розподіляються по відкритій місцевості, тому вони можуть легко стати ціллю і фізичне руйнування датчиків може також зазнати вторгнення.

Зважаючи на характер БСМ, зловмисники хочуть отримати прибуток за допомогою обмежень БСМ, таких як апаратне забезпечення сенсорних

вузлів, і вони намагаються зробити їх необслуговуючими, перевантажуючи їх. Ще один підхід атаки - на фізичному рівні. Зловмисники також хочуть домогтися атак заклинювання та підриву. У роботі [20] в якості контрзаходу атаці заклинювання описано, що протокол відображення вузлів забезпечує ситуаційну обізнаність у сусідніх вузлах, щоб помітити атаку заклинювання за допомогою розповсюдження повідомлень. Окрім нападу фізичного рівня, зловмисники можуть пошкодити датчики, а щоб уникнути цієї атаки, користувачі намагаються замаскувати датчики у навколишньому середовищі.

2. Атаки неправильного спрямування (Misdirection)

Атаки неправильного спрямування змінюють інформацію про маршрутизацію БСМ і вони негативно впливають на загальну систему БСМ. Мета атаки - пересилання даних (повідомлення) по невірному шляху. На рис. 2.1 атака неправильного спрямування показана як атака мережевого рівня. У роботі [21] описано, що важливо зрозуміти, чи є якесь неправильне спрямування чи ні. Цього можна досягти, виконавши деякий аналіз та тести, обчисливши пропускну здатність БСМ. Існують деякі методи виявлення нападів неправильного спрямування. Ці методи коротко описані нижче:

- Використання результатів хешованих пакетів даних. Цей метод не потребує додаткової енергії.
- Створення та використання механізму аутентифікації між вузлами приймача та передавача.
- Використання безпечної багато-скачкової маршрутизації. Але виявити шкідливі вузли не вдається.

3. Атака вибіркової переадресації (Selective Forwarding)

Атака вибіркової переадресації - це одна з атак мережевого рівня. Цей тип атак впливає на мережевий трафік, вважаючи, що всі вузли, що беруть участь у мережі, надійні для пересилання повідомлення. При атаці вибіркової переадресації зловмисні вузли просто відкидають певні повідомлення, а не

пересилають кожне повідомлення. Після того, як зловмисний вузол вибрав повідомлення, він зменшує затримку та обманює сусідні вузли тим, що вони перебувають у більш короткому маршруті. Ефективність цієї атаки залежить від двох факторів. По-перше, місцеположення зловмисного вузла, чим ближче він до базових станцій, тим більше трафіку він буде залучати. По-друге - відсоток повідомлень, які він скидає. Коли вибірковий сервер пересилання відкидає більше повідомлень і передає менше, він зберігає свій рівень енергії, залишаючись таким чином потужним для обману сусідніх вузлів.

4. Атака на приймач (Sinkhole Attack)

Під час Sinkhole атаки зловмисник домовляється з вузлом або вводить в мережу підроблений вузол і використовує його для здійснення атаки. Зловмисник прослуховує запити маршрутів вузлів і намагається переконати, що у нього найкоротший шлях до базової станції [22]. Коли узгоджений вузол або підроблений вузол досягають залучення мережевого трафіку, він створює атаку. Sinkhole атака описується як атака канального рівня (рис. 2.1). Після досягнення зловмисного вузла (узгодженого, введеного вузла) вони можуть робити все, що завгодно, наприклад, скидувати всі пакети, скидувати вибрані пакети, змінювати вміст пакетів. У [22] методи виявлення класифікуються на п'ять груп (на основі правил, на основі аномалій, статистичні методи управління криптографічними ключами та гібридні системи) та детально пояснюються. Контрзаходи атаці згруповано у вигляді узгодженості даних - підхід на основі інформації про мережевий потік, схема моніторування кількості переходів, використання моніторингу вузлів центрального процесору, підхід на основі мобільного агента, використання алгоритму дайджесту повідомлень, і ці контрзаходи описані детально [22].

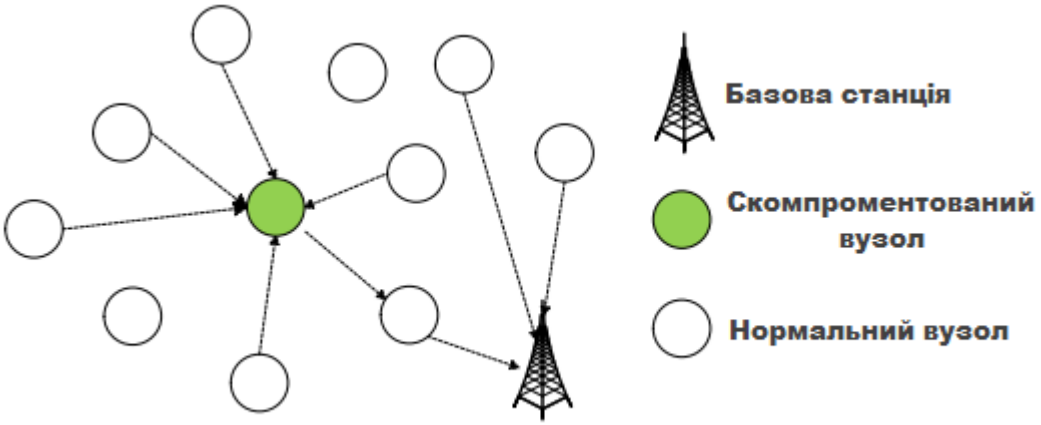

Рисунок 2.2 Модель Sinkhole атаки

5. Атака Сибіл (Sybil)

Sybil атака описується як шкідливий вузол, який незаконно приймає декілька ідентифікаторів. У БСМ всі вузли повинні працювати разом з іншими вузлами для досягнення заданого порядку. При sybil атаці ціллю є порушити цю співпрацю. Типи sybil атак описані в трьох вимірах, і пояснюється, що для виявлення sybil-атаки дуже важливо розуміти, який тип системи має sybil атака. Види sybil атак: пряма та непряма комунікація, сфабриковані та викрадені ідентифікаційні дані, одночасна та неодночасна атака. За допомогою цієї атаки шкідливий вузол може націлюватися на протокол маршрутизації, процеси співпраці та використовуваний механізм виявлення [23].

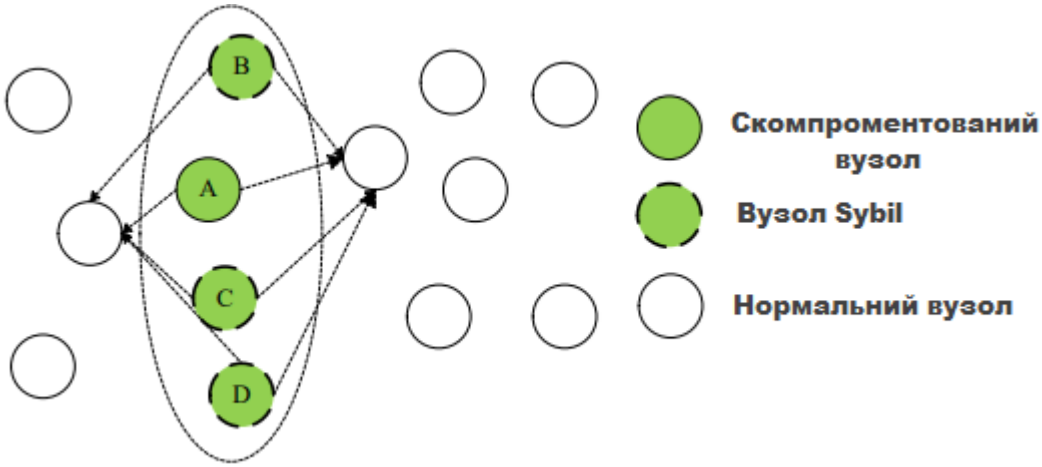

Рисунок 2.3 Модель атаки Sybil

6. Атака червоточини (Wormhole Attack)

Атака червоточини є атакою канального рівня, і може впливати на мережу без знання криптографічних методів, реалізованих у БСМ. При атаках червоточини зловмисник, розташований ближче до базової станції, може повністю порушити трафік, тунелюючи повідомлення через канал з маленькою затримкою. Тут зловмисник переконує вузли, які перебувають поруч, що вони ближче до базової станції. Це створює провал, оскільки супротивник з іншого боку провалу забезпечує кращий маршрут до базової станції.

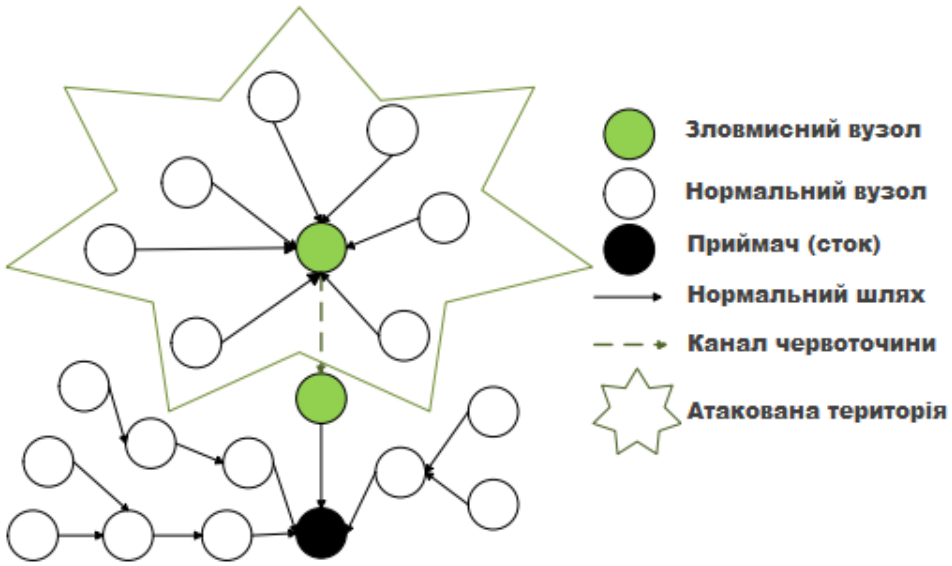

Рисунок 2.4 Концептуальний погляд на Wormhole атаку

7. Hello flood атаки

У мережевих структурах протоколам маршрутизації потрібні деякі пакети, які називаються "пакети HELLO", щоб знайти сусідів. В Hello flood атаках широкомовне повідомлення з більшою потужністю передачі робить вигляд, що повідомлення HELLO надходить з базової станції. Вузли прийому повідомлень припускають, що вузол передачі повідомлень HELLO є найближчим, і вони намагаються надіслати всі свої повідомлення через цей вузол. У цьому типі атак усі вузли реагуватимуть на HELLO потоки та

витрачають енергію. Реальна базова станція також транслюватиме подібні повідомлення, але відповідатиме на нього лише декілька вузлів. Можливими рішеннями для виявлення атак цього типу можуть бути використання двосторонньої перевірки посилань, безпечна маршрутизація з декількома шляхами та використання декількох базових станцій [24].

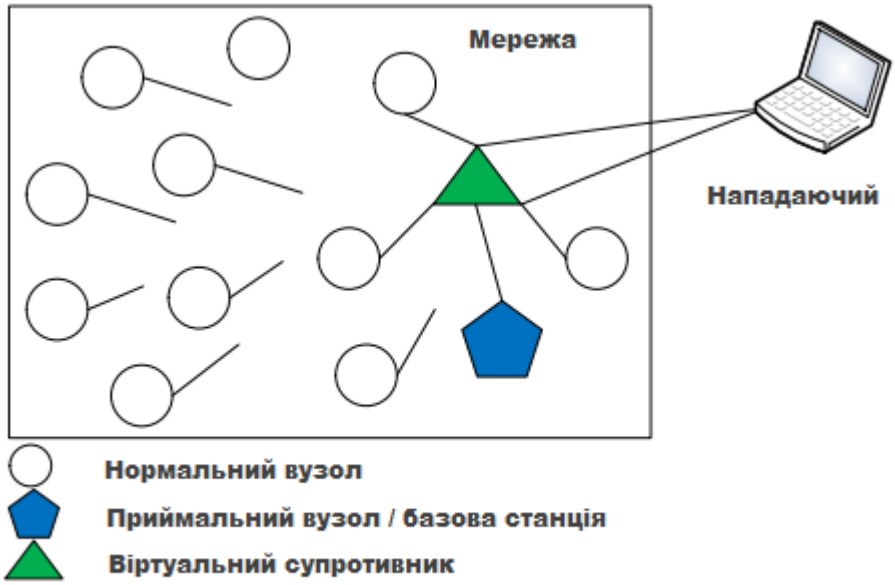

Рисунок 2.5 Концептуальний погляд на Hello flood атаку

2.2 Організація безпеки в бездротовій сенсорній мережі

Однією з ключових особливостей БСМ є її багато-скачкові розподілені операції, що додають більше складності щодо виявлення та запобігання атакам безпеки. У багато-скачковому розподіленому середовищі дуже важко визначити зловмисників або шкідливі вузли. Багато механізмів виявлення та запобігання атакам безпеки розроблені для БСМ; однак більшість існуючих рішень здатні обробляти лише декілька атак безпеки. Наприклад, більшість протоколів захищеної маршрутизації призначені для протидії декільком атакам безпеки [25].

Аналогічно нові механізми доступу до середовища розроблені для вирішення проблеми прихованого вузла. Механізми шифрування призначені для захисту даних від пасивних атак. Отже, можна сказати, що існує потреба

у розробці механізмів, здатних виявляти та запобігати безлічі атак безпеки на БСМ. Система виявлення вторгнень (IDS) є одним з можливих рішень цієї проблеми.

Вторгнення – це, в основному, будь-яка протиправна діяльність, яка здійснюється зловмисниками з метою завдати шкоди мережевим ресурсам або сенсорним вузлам. IDS є механізмом виявлення такої протиправної злочинної діяльності [25]. Основні функції IDS - відстежувати діяльність користувачів та поведінку мережі на різних рівнях.

Єдиний ідеальний захист є неможливим у бездротових мережах, оскільки завжди існують деякі архітектурні недоліки, програмні помилки чи недоліки в проекті, які можуть порушити зловмисників. Найкраща практика для забезпечення захисту бездротових мереж полягає в тому, щоб реалізувати множину механізмів безпеки; саме тому IDS є важливим у бездротових мережах. Це розглядається як пасивний захист, оскільки вона не призначена для запобігання нападів; натомість вона вчасно сповіщає мережевих адміністраторів про можливі атаки, щоб зупинити або зменшити вплив атаки. Точність виявлення вторгнень зазвичай вимірюється з точки зору помилкових спрацьовувань (помилкових сигналів тривоги) та помилкових негативів (атак не виявлено), де IDS намагається мінімізувати обидві ці умови [25].

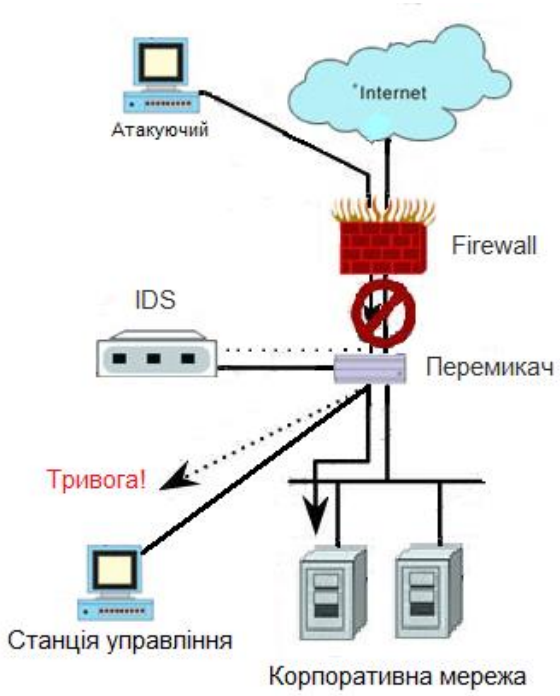

Рисунок 2.6 Організація безпеки в БСМ

2.3 Концепція систем запобігання вторгнень і виявлення вторгнень

Система запобігання вторгнень (IPS) - це вбудований пристрій, який блокує атаки, перш ніж вони зможуть досягти своєї мети. У більш широкому розумінні IPS здійснює загальну перевірку пакетів, забезпечуючи цілий спектр функцій завдяки цій глибині аналізу та класифікації трафіку [26]. Взагалі IPS класифікується на хостові IPS та мережеві IPS.

Хостові IPS - це програмне забезпечення, яке знаходиться на окремих системах, таких як сервери, робочі станції або ноутбуки. Трафік, що надходить в цю систему або виходить з неї, перевіряється, і поведінка програм і операційної системи може бути перевірена на наявність ознак атаки. При виявленні атаки програмне забезпечення Host IPS або блокує атаку на рівні мережевого інтерфейсу, або видає команди програмі чи операційній системі для припинення поведінки, ініційованої атакою [26].

Пристрої мережевих IPS розгортаються в один ряд із захищеним сегментом мережі. Усі дані, що передаються між захищеним сегментом і рештою мережі, повинні проходити через пристрій мережевої IPS. Коли трафік проходить через пристрій, він перевіряється на наявність нападу.

Коли атака ідентифікується, мережева IPS відкидає або блокує несанкціоновані дані від проходження через систему до ймовірної жертви, таким чином блокуючи атаку [26].

Адміністратори БСМ намагаються уникати атак безпеки і використовують деякі механізми захисту та виявлення. У таких підходах до управління безпекою система виявлення вторгнень (IDS) є другою лінією безпеки. IDS може бути визначений як програмний або апаратний пристрій, який здійснює моніторинг мережі для виявлення внутрішніх або зовнішніх кібератак. Цілі IDS - виявлення атак, запобігання нападів шляхом забезпечення стримування зловмисників, збирання доказів з мережі, інформування про ситуацію, виконання політики щодо зв'язку. Класично відома структура IDS зображена на рис. 2.7. Архітектура IDS, як зображено на рис. 2.7 [27], містить чотири основні компоненти:

Рисунок 2.7 Структура системи виявлення вторгнень

- Датчик: збирає дані з моніторингової системи.

- Детектор (Analyze Engine): аналіз зібраних даних для виявлення вторгнень.
- База знань: допомагає детектору виявити, подаючи підписи атак
- Компонент відповіді: Керує діями реагування на атаки.

IDS може працювати в багатьох режимах, наприклад, в автономному режимі та в кооперативному кластерному режимі [28]. Автономна IDS працює на кожному вузлі для виявлення небажаних дій. Кооперативні IDS на основі кластера є найбільш поширеним, в якому кожен вузол контролює діяльність та роботу своїх сусідів та навколишніх вузлів; у разі виявлення будь-якої зловмисної активності, це повідомляється голові кластера.

IDS класифікуються як мережева система виявлення вторгнень (NIDS) та хост-система виявлення вторгнень (HIDS). Ця класифікація проводиться відповідно до методики моніторингу системи. HIDS знаходиться на певному комп'ютері і відстежує вторгнення, які можуть бути на цій машині. NIDS знаходиться в розподіленій мережі і відстежує мережевий трафік для виявлення вторгнень, які можуть бути в цій мережі. Датчики NIDS можуть бути в будь-якому місці мережі. На сьогоднішній день поєднання NIDS та HIDS є актуальною тенденцією. Цей підхід називається гібридною системою. Існує два основних підходи до виявлення вторгнень. Ці підходи також можна розділити і на два методи. Методи називаються виявлення аномалії та виявлення зловживань.

1. Виявлення аномалій

Системи виявлення аномалій намагаються виявити мережеві дії, які відрізняються від звичайної поведінки системи. Виявлення аномалій має деякі методи, такі як мобільний агент, статистика, аналіз даних, нейронні мережі. Девіз виявлення аномалії - це "аномалії не є нормальними". Виявлення аномалії добре працює для невідомих атак, але іноді рівень помилкових сповіщенн може бути високим. Як показано на рис. 2.8, IDS, що працює з технікою виявлення аномалії, відповідно отримує дані аудиту, вивчає дані, щоб вирішити, чи є аномалія чи ні, і нарешті, якщо аномалія є,

вона попереджає систему відповідним повідомленням [29]. Іноді не вдається виявити відомі атаки безпеки. Причина полягає в тому, що IDS на основі аномалій не підтримують жодної бази даних, але вони постійно відстежують схеми трафіку або активність системи.

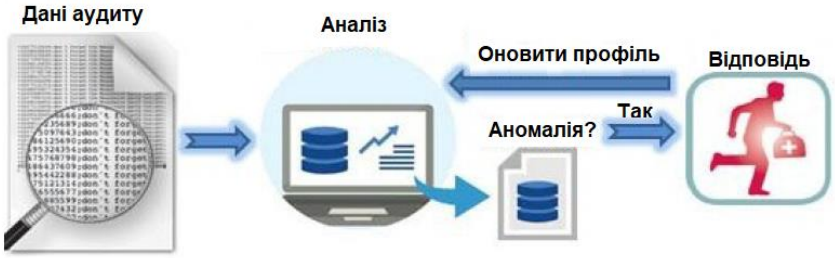

Рисунок 2.8 Основна система виявлення аномалії

2. IDS на основі підписів

IDS, що використовує цю методику, має базу знань, що включає підписи відомих атак та слабких місць системи. Під підписом розуміють характеристики (профілі) відомих атак зловмисника. IDS порівнює поточну роботу з кожним профілем, що зберігається. При збігу з одним з них, механізм виявлення вторгнення сповіщає про це. Такий метод дуже успішно виявляє відомі напади, але недолік полягає в тому, що він не дозволяє виявити новий (невідомий) вид атаки; [28].

У [29] визначено п’ять правил таких як правило заклинювання (jamming rule), правило інтервалу, правило цілісності, правило повторної передачі та правило радіопередачі для виявлення заклинювань, змінених пакетів, вибіркового пересилання та флуду.

Алгоритм використовує три фази:

1. На фазі збору даних важливі повідомлення збираються та зберігаються для подальшого аналізу.

2. На фазі застосування правила збережені дані перевіряються за допомогою правил, якщо це не вдається, то виникає помилка;

3. На фазі виявлення вторгнень кількість виниклих помилок порівнюється з випадковими збоями в мережі. Якщо кількість помилок велика, то система виявлення вторгнень видає попереджувальне повідомлення.

У [30], локальний агент використовує метрику порогових показників на вузлі, тоді як центральний агент використовує методи дерева рішень на базовій станції. Якщо локальний агент виявляє будь-яку аномальну активність, він подає попереджувальний сигнал тривоги центральному агенту. Центральний агент аналізує інформацію сигналу, надану місцевим агентом, якщо попередження підтверджено, він передає повідомлення всім локальним агентам про своє рішення.

У роботі [31] реалізовано мережу на комбінації правил, зворотного розповсюдження та теорії адаптивного резонансу. Алгоритм реалізований на сенсорних вузлах, щоб виявити, атакується пакет чи ні. Голова кластера реалізує алгоритм зворотного розповсюдження, який поєднує модель виявлення аномалії та виявлення зловживань для пошуку атак. Вихідні дані як моделі, заснованої на правилах, так і моделі зворотного розповсюдження, передаються мережі адаптивного резонансу, щоб знайти типи атак, і він попереджає адміністратора про необхідність подальших дій.

Більшість існуючих IDS зосереджуються на виявленні атак мережевого рівня та пропускають виявлення атак інших рівнів [28]. В деяких випадках, атаки одного рівня можуть нанести атаки іншим рівням. Наприклад, компромісна атака вузла фізичного рівня може скидати пакети, що є атакою мережевого рівня [28]. Отже, міжрівнева IDS повинна використовуватися для виявлення атак фізичного рівня, канального рівня та мережевого рівня.

Висновки до розділу

У WSN загрози безпеці сильніше відрізняються від дротових та бездротових мереж. Ці відмінності обумовлені типовими властивостями WSN. Енергія є важливим обмеженням для WSN, і крім трьох компонентів безпеки (конфіденційність, цілісність та доступність), є новий базовий аспект - енергія.

Розглянуто кібератаки, які відбуваються в бездротових сенсорних мережах: атаки на відмову в обслуговуванні (DoS), атаки неправильного спрямування (Misdirection), атака вибіркової переадресації (Selective Forwarding), атака на приймач (Sinkhole Attack), атака Сибіл (Sybil), атака червоточини (Wormhole Attack), Hello flood атаки.

Визначено організацію безпеки в бездротовій сенсорній мережі. Багато механізмів виявлення та запобігання атакам безпеки розроблені для БСМ; однак більшість існуючих рішень здатні обробляти лише декілька атак безпеки. Найкраща практика для забезпечення захисту бездротових мереж полягає в тому, щоб реалізувати множину механізмів безпеки; саме тому IDS є важливим у бездротових мережах.

Проведено аналіз систем запобігання вторгнень і виявлення вторгнень. Система запобігання вторгнень (IPS) - це вбудований пристрій, який блокує атаки, перш ніж вони зможуть досягти своєї мети. IPS здійснює загальну перевірку пакетів, забезпечуючи цілий спектр функцій завдяки цій глибині аналізу та класифікації трафіку. Система виявлення вторгнень (IDS) є другою лінією безпеки. Існує два основних підходи до виявлення вторгнень: виявлення аномалії та IDS на основі підписів.

Більшість існуючих IDS зосереджуються на виявленні атак мережевого рівня та пропускають виявлення атак інших рівнів. В деяких випадках, атаки одного рівня можуть нанести атаки іншим рівням.

РОЗДІЛ 3
МАШИНА ЕКСТРЕМАЛЬНОГО НАВЧАННЯ

Машини екстремального навчання (ELM) - стала гарячою зоною досліджень протягом останніх років, що пояснюється зростаючою науково-дослідною діяльністю та значним внеском численних дослідників у всьому світі. Нещодавно стало відомо, що низка помилкових уявлень та непорозумінь розсіюється щодо взаємозв'язків між ELM та деякими попередніми роботами.

У цій роботі зазначається, що (1) теорії ELM вдається вирішити відкриту проблему, яка впродовж 60 років спантеличує нейронні мережі, машинне навчання та нейронаукові спільноти: чи потрібно налаштовувати приховані вузли / нейрони на навчання, і доведено, що на відміну від загальновідомих та загальноприйнятих принципів навчання нейронної мережі, приховані вузли / нейрони не потребують ітеративного налаштування на широкі типи нейронних мереж та моделей навчання (ряди Фур'є, біологічне навчання тощо).

На відміну від теорій ELM, жодна з цих ранніх робіт не дає теоретичних основ для нейронних мереж з прямим зв’язком із випадково схованими вузлами; (2) ELM пропонується як для узагальненої мережі прямого зв’язку з одним прихованим рівнем, так і для мережі прямого зв’язку з декількома прихованими рівнями (включаючи біологічні нейронні мережі); (3) для вивчення особливостей кластеризації, регресії та (бінарної / багатокласової) класифікації пропонується ELM на основі однорідної архітектури. (4) У порівнянні з ELM, SVM і LS-SVM, як правило, надають субоптимальні рішення, і SVM і LS-SVM також не враховують представлення функцій прихованих рівнів мереж з прямим зв’язком з декількома прихованими рівнями.

3.1 Концепція машини екстремального навчання

Незважаючи на те, що зв'язки та відмінності між машинами екстремального навчання (ELM) та більш ранніми роботами (наприклад,

Шмідт [32] та RVFL [33]) були з'ясовані в [34], останнім часом деякі дослідники наполягають на тому, що ці ранні роботи - це «витоки» ELM та по суті такі ж, як і попередні роботи, і, таким чином, далі заявляли, що немає необхідності в новому терміні машин екстремального навчання (ELM). Кінцева мета дослідження - знайти істинність природних явищ і просунути дослідження вперед, замість того, щоб стверджувати, що вони занесені до «витоків».

Інакше багато ранніх робіт не мали б мати власних термінів, а натомість майже всі повинні були просто називатись "нейронними мережами з прямим зв'зком". Таке непорозуміння щодо ігнорування потреб нових термінів насправді перешкоджає творчому підходу дослідників та їхньому духу розповідати правду та відмінності в дослідженні. Так само немає нічого поганого в тому, щоб мати нові терміни для варіантів ELM (з вузлами рядів Фур'є), а також ELM з LMS, що називається алгоритмом No-Prop [33].

Для більш чіткого розуміння ELM, краще проаналізувати ELM в аспектах його філософії, теорій, мережевої архітектури, типів мережевих нейронів та його цілей та алгоритмів навчання.

Як зазначено у [34], "Екстремальний" означає вихід за рамки звичайних методів штучного навчання та рух до навчання, подібне інтелектуальному. ELM прагне подолати бар'єри між звичайними методами штучного навчання та біологічним механізмом навчання. "Машина екстремального навчання (ELM)" являє собою набір методів машинного навчання (включаючи мережі прямого зв’язку з одним прихованим рівнем), в яких приховані нейрони не потрібно налаштовувати з урахуванням узагальнення теорії нейронної мережі, теорії управління, теорії матриць та теорії лінійних систем. Випадкове генерування прихованих вузлів - одна з типових реалізацій, яка гарантує, що "приховані нейрони не потрібно налаштовувати" в ELM; однак, існує також багато інших реалізацій, таких як ядра, SVD та локальні рецептивні поля [34]. Вважається, що ELM відображає істинність деяких біологічних механізмів навчання. Її ефективність на основі машинного

навчання була підтверджена в 2004 році [35], а її універсальна здатність апроксимації (для " узагальнених SLFN ", в яких прихований вузол може бути підмережею декількох вузлів та / або майже з будь-якими нелінійними частково-неперервні нейронами (хоча їх точне математичне моделювання / формула / форми може бути невідоме людям)) було доведено теоретично у 2006–2008 роках [36]. Його конкретні біологічні дані згодом з'являються у 2011–2013 роках [37].

ELM призначений не тільки для "узагальнених" мереж прямого зв’язку з одним прихованим рівнем, але і для "узагальнених" мереж прямого зв’язку з прихованим рівнем, в якому вузол може бути підмережею, що складається з інших прихованих вузлів [36]. Один прихований рівень ELM також охоплює широкі типи нейронних мереж, включаючи, але не обмежуючись ними, сигмоподібні мережі та мережі RBF.

Стиснення, вивчення функцій, кластеризація, регресія та класифікація є основами для машинного навчання та машинного інтелекту. ELM направлена на реалізацію цих п'яти основних операцій / ролей навчання в однорідних архітектурах ELM (див. рис. 3.1).

Рисунок 3.1 Основні операції / ролі ELM

Не дивлячись на те, що у 1950-1990-х роках було декілька спроб на випадкові сигмоїдні приховані нейрони та / або RBF-нейрони, цей тип реалізацій насправді не «взлетів», за винятком RVFL [38] з кількох причин:

1. Загальне розуміння і принцип полягає в тому, що приховані нейрони різних типів нейронних мереж потребують налаштування.

2. Відсутній теоретичний аналіз, крім RVFL.

3. У біологічному навчанні бракує сильної мотивації, за винятком персептрону Розенблатта.

Теорії ELM вдалося вирішити складне питання: "Чи можуть бути випадковим чином генеровані широкі типи нейронних мереж (включаючи біологічні нейронні мережі) із широкими типами прихованих вузлів / нейронів (майже будь-які нелінійні частково-неперервні вузли)". Хоча ELM прагне працювати як з мережами прямого зв’язку з одним прихованим рівнем (SLFN), так і з мережами прямого зв’язку з декількома прихованими рівнями, його теорії в основному зосереджуються на випадках SLFN протягом останніх 10 років.

3.2 Можливість універсального наближення

Власне кажучи, в жодній з цих більш ранніх робіт (наприклад, Баум [31] та Шмідт [32], RVFL [33]) теоретично не розглядається питання про те, чи можна використовувати випадкові приховані вузли в їхніх специфічних сигмоподібних або RBF-мережах, не кажучи вже про широкий тип мереж, охоплених теоріями ELM. [37] RBF-мережа Лоу не використовує фактор випадкового впливу, хоча центри їх вузлів RBF генеруються випадковим чином. Слід налаштувати фактори впливу на основі додатків. Іншими словами, в мережі RBF використовуються напіввипадкові вузли RBF [37].

І Баум, і Шмідт зосередили увагу на емпіричному моделюванні конкретних мережевих архітектур (конкретний випадок моделей ELM). Наскільки відомо, обидві попередні роботи не мають теоретичного аналізу, не кажучи вже про суворий теоретичний доказ. Хоча інтуїтивно кажучи, Ігельник і Пао намагались довести універсальну апроксимативну здатність RVFL, проаналізовану в [39], насправді Ігельник і Пао довели лише універсальну апроксимативну здатність RVFL тільки тоді, коли використовуються напіввипадкові сигмоїди та RBF приховані вузли, тобто вхідні ваги a_i генеруються випадковим чином, тоді як зміщення прихованого вузла b_i розраховується на основі навчальних зразків x_i та вхідних ваг a_i.

На противагу цьому, теорії ELM показали, що майже будь-які нелінійні частково-безперервні випадкові приховані вузли (включаючи сигмоподібні та RBF-вузли, згадані в цих попередніх роботах, але також включаючи вейвлет, ряди Фур'є та біологічні нейрони) можуть використовуватися в ELM, і отримані мережі мають універсальні апроксимаційні можливості [31]. На відміну від напів-випадкових сигмоїдних та RBF прихованих вузлів, що використовуються у доказі RVFL [32], у якому деякі параметри не генеруються випадковим чином, фізичний сенс випадкових прихованих вузлів у теоріях ELM полягає в тому, що всі параметри прихованих вузлів генеруються випадковим чином незалежно від навчальних зразків, наприклад, як випадкові вхідні ваги a_i, так і зміщення b_i для адитивних

прихованих вузлів, або обох центрів a_i та коефіцієнта впливу b_i для мереж RBF, параметрів для рядів Фур'є та вейвлетів тощо. Теорії ELM вперше показали, що всі приховані вузли / нейрони можуть бути не тільки незалежними від навчальних зразків, але й незалежними один від одного в широких типах нейронних мереж і математичних серій / розширень, а також у механізмі біологічного навчання [36].

Визначення 3.1 [36] Вихідне відображення прихованого рівня $h(x) = [h_1(\mathrm{x}), \dots, h_L(\mathrm{x})]$ називається відображенням випадкових ознак ELM, якщо всі його приховані параметри вузла генеруються випадковим чином відповідно до будь-якої ймовірності розподілу безперервної вибірки, де $h_i(x) = G_i(a_i, b_i, x), i = 1, \dots, L$ (кількість нейронів у прихованому рівні).

Різні приховані вузли можуть мати різні вихідні функції G_i. У більшості додатків, для спрощення, для всіх прихованих вузлів можна вибрати однакові вихідні функції, тобто $G_i = G_j$ для всіх $i, j = 1, \dots, L$.

Теорема 3.1 (Можливість універсального наближення [36] Якщо в якості функції активації задана будь-яка непостійна частково-безперервна функція, та якщо налаштування параметрів прихованих нейронів могло б привести до того, що SLFN наблизяться до будь-якої цільової безперервної функції *f(x)*, то послідовність $\{h_i(x)\}_{i=1}^{L}$ може бути генерована випадковим чином відповідно до будь-якої ймовірності безперервного розподілу, та $\lim_{L\to\infty} \left\| \sum_{i=1}^{L} \beta_i h_i(x) - f(x) \right\| = 0$ виконується з вірогідністю один з відповідною вихідною вагою β.

Можливість класифікації

Крім того, теорії ELM також доводять можливість класифікації широких типів мереж із випадковими прихованими нейронами, і такі теорії не вивчалися в цих попередніх роботах.

Теорема 3.2 (Можливість класифікації) Якщо в якості функції активації задана будь-яка непостійна частково-безперервна функція, та якщо налаштування параметрів прихованих нейронів може призвести до того, що SLFN наблизяться до будь-якої цільової безперервної функції *f(x)*, тоді SLFN

з випадковим відображенням прихованого рівня *h(x)* можуть відокремитись довільні непересічні ділянки будь-якої форми.

Складно мати справу з декількома прихованими рівнями ELM безпосередньо, не маючи комплексних рішень одного прихованого рівня ELM. Таким чином, за останні 10 років більшість робіт ELM були зосереджені на "узагальнених" мережах прямого зв’язку з одним прихованим рівнем (SLFN).

"Узагальнені" мережі прямого зв’язку з одним прихованим рівнем (SLFN)

Дослідження Шмідта [1] зосереджується на сигмоподібних мережах, дослідження Пао [32] фокусується на RVFL (з сигмоподібними або RBF-вузлами). Обидва мають стандартний один прихований рівень, що не є "узагальненою" мережею прямого зв’язкуз одним прихованим рівнем (SLFN), вивченою в ELM. Аналогічно SVM [39], нейронна мережа прямого зв’язку з випадковими вагами, запропонована у Шмідта вимагає зміщення у вихідному вузлі для того, щоб поглинути системну помилку, оскільки його можливість універсального наближення до випадкових сигмоподібних вузлів не було доведено, коли було запропоновано:

$$f_L(x) = \sum_{i=1}^{L} \beta_i g_{sig}(a_i \times x + b_i) + b, \quad \text{де } g_{sig}(x) = \frac{1}{1+\exp(-x)}$$

(3.1)

І QuickNet, і RVFL мають прямий зв'язок між вхідним вузлом і вихідним вузлом:

$$f_L(x) = \sum_{i=1}^{L} \beta_i g_{sig\ or\ RBF}(a_i, b_i, x) + \alpha x$$

(3.2)

ELM пропонується для "узагальнених" мереж прямого зв’язку з одним прихованим рівнем та математичних рядів / розширень (які можуть навіть не бути звичайними нейронними мережами, такими як вейвлет та ряди Фур'є):

$$f_L(x) = \sum_{i=1}^{L} \beta_i G(a_i, b_i, x)$$

(3.3)

Основний ELM призначений для узагальненого SLFN, на відміну від повністю підключених мереж у тих попередніх роботах, у ELM є три рівні випадковості (рис. 3.2):

1. Повністю підключені параметри прихованого вузла генеруються випадковим чином.

2. З'єднання можна генеруватися випадковим чином, не всі вхідні вузли підключені до певного прихованого вузла. Можливо, лише деякі вхідні вузли в якомусь локальному полі підключені до одного прихованого вузла.

3. Сам по собі прихований вузол може бути підмережею, утвореною кількома вузлами, які формують локальні рецептивні поля та функції об’єднання, і, таким чином, призводить до вивчення локальних особливостей. У цьому сенсі деякі локальні частини одного ELM можуть містити декілька прихованих рівнів.

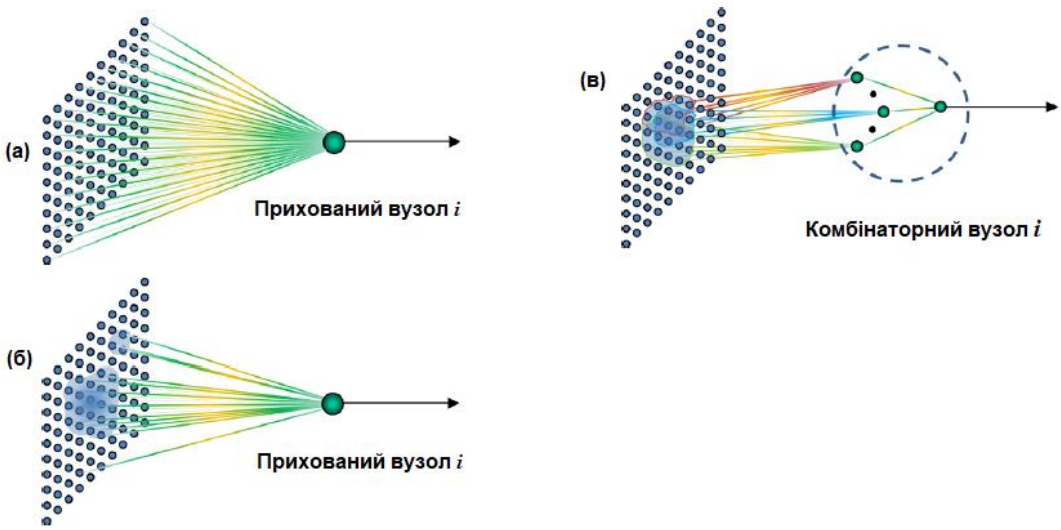

Рисунок 3.2 Теорії ELM показують, що широкі типи прихованих вузлів можуть бути мережами прямого зв'язку з одним прихованим рівнем. "Узагальнена SLFN", на яку посилається ELM, означає підмережу з декількох вузлів. а) Прихований вузол у повному зв'язку в ELM. б) Прихований вузол локального зв'язку \ випадкового з'єднання в ELM. в) Комбінаторний вузол з декількох вузлів в ELM *i*

На відміну від Шмідта та Пао, у якому кожен вузол є лише сигмоїдним або RBF-вузлом, кожен прихований вузол в ELM може бути підмережею

інших вузлів, в яких функціональне навчання може бути реалізовано ефективно.

Згідно теорій ELM [36], ELM SLFN включають, але не обмежуються ними:

1. Сигмоїдні мережі
2. Мережі RBF
3. Порогові мережі
4. Тригонометричні мережі
5. Системи нечітких висновків
6. Повністю складні нейронні мережі
7. Мережі високого порядку
8. Мережі поліномічного хребта
9. Вейвлет-мережі
10. Ряди Фур'є
11. Біологічні нейрони, моделювання / форми яких може бути невідома тощо.

Мережі прямого зв’язку з декількома прихованими рівнями

Однак, на відміну від Шмідта та RVFL, який працює лише для мереж прямого зв’язку з одним прихованим рівнем, кінцевим принципом ELM є: приховані вузли широких типів мереж з декількома прихованими рівнями не потребують налаштування (Рис. 3.3). Хоча багаторівневі концепції ELM були наведені в теоріях ELM у 2007 році, вони до недавнього часу не використовувалися. По суті:

1. Розенблат намагався перенести вивчену поведінку від підготовлених щурів до наївних щурів шляхом ін'єкції мозкових екстрактів, що може не враховувати той факт, що різні рівні нейронів можуть грати різну роль. На відміну від концепції персептрона Розенблатта, вважається, що неможливо створити всі рівні випадковим чином. Якщо всі рівні в багаторівневій мережі генеруються випадковим чином, корисна інформація

може не проходити через два або більше чисто випадкових прихованих рівнів. Однак, кожен базовий ELM може бути використаний у кожному прихованому рівні, приховані нейрони не потрібно налаштовувати за рівнями і різний рівень може мати різні цілі (з точки зору п'яти основних операцій ELM: стиснення, вивчення функцій, кластеризація, регресія та класифікація).

2. Значення того, що приховані вузли не потрібно налаштовувати, є подвійними:

- Приховані вузли можуть генеруватися випадковим чином.
- Хоча приховані вузли не потрібно генерувати випадковим чином, їх також не потрібно налаштовувати. Наприклад, прихований вузол у наступному рівні може бути просто лінійною сумою або нелінійним перетворенням деяких випадково згенерованих вузлів на попередньому рівні. У цьому випадку деякі вузли генеруються випадковим чином, а деякі - ні, але жоден з них не налаштований [31].

3. Кожна окрема ELM може мати справу з стисненням, вивченням функцій, кластеризацією, регресією чи класифікацією. Таким чином, можна побудувати однорідні ієрархічні блоки ELM. Наприклад, одна ELM як вивчення функцій, наступна ELM працює як класифікатор. У цьому випадку маємо два приховані рівні ELM, в цілому це не генерується випадковим чином, і він впорядкований, але приховані вузли на кожному рівні не потрібно налаштовувати (наприклад, генерувати випадковим чином або явно задавати / обчислювати (рис. 3.3а).

4. ELM-фрагменти, які виконують функції навчання або кластеризації ролей, також можуть використовуватися для зв’язку різних моделей навчання. Або як ціла мережа, деякі рівні навчаються по ELM, а деякі – по іншими моделями (рис. 3.4).

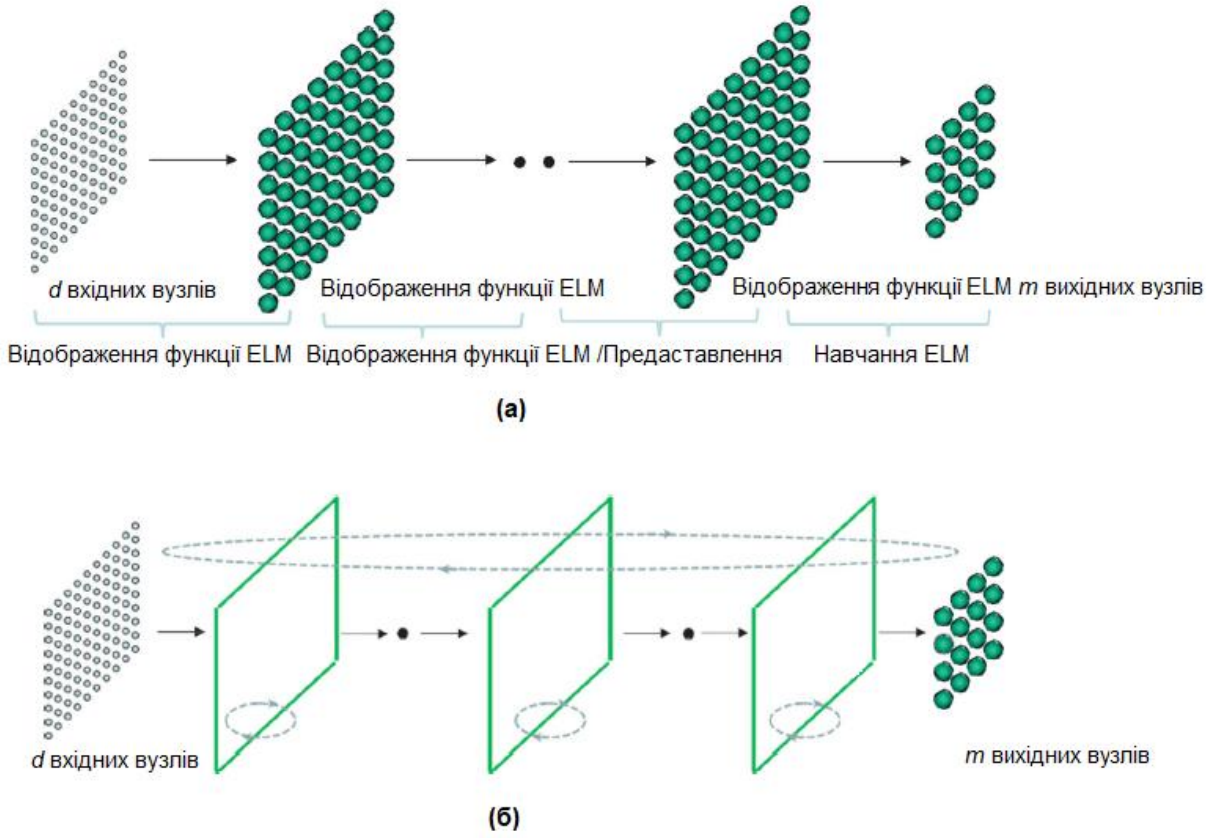

Рисунок 3.3 Порівняння ієрархічного ELM та глибокого навчання: кожен фрагмент ELM утворює один прихований шар, а прихований вузол у деяких прихованих шарах може бути підмережею декількох нейронів

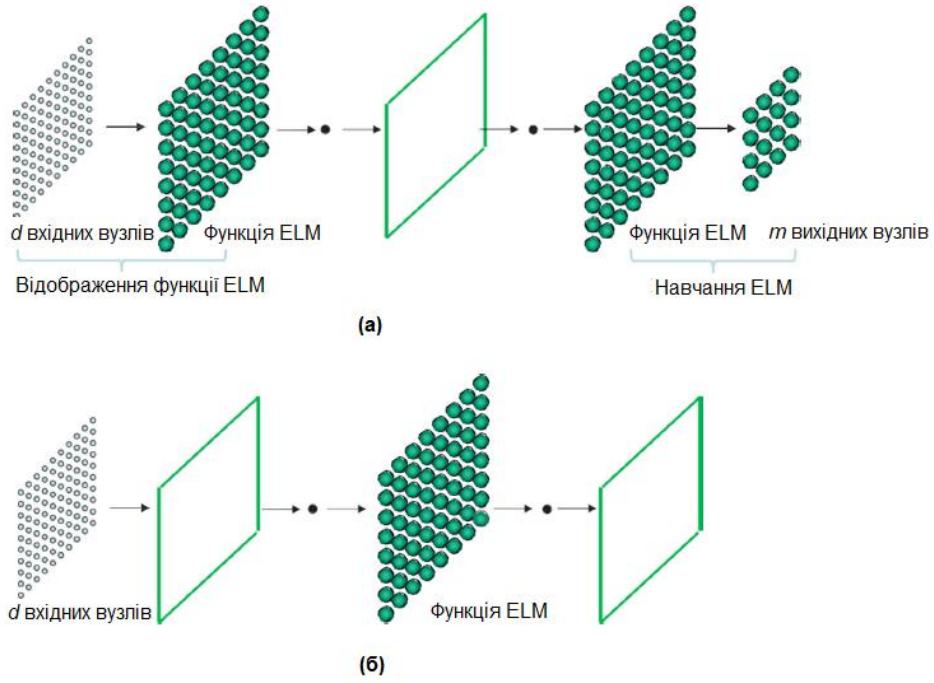

Рисунок 3.4 Фрагмент ELM працює з різними моделями навчання: Однак кожен фрагмент ELM як основний елемент навчання може бути включений до інших моделей навчання. а) Інші моделі навчання працюють між різними

фрагментами ELM. б) Фрагменти ELM працюють між різними моделями навчання

3.3 Зв'язок та відмінності серед ELM, глибоке навчання та SVM / LS-SVM

ELM відрізняється від глибокого навчання тим, що приховані нейрони всього ELM не потрібно налаштовувати. Завдяки різній ролі ELM у функціонуванні та кластеризації, ELM може використовуватися в якості попередніх рівнів в багаторівневих мережах, в яких наступні рівні навчаються іншими методами, такими як глибоке навчання (рис. 3.5). Спочатку SVM був запропонований Кортесом та Вапником для обробки багаторівневих мереж прямого зв’язку [39], що передбачає, що коли немає алгоритму для навчання багаторівневої мережі, функцію виводу останнього прихованого рівня можна розглядати як $\phi(x)$.

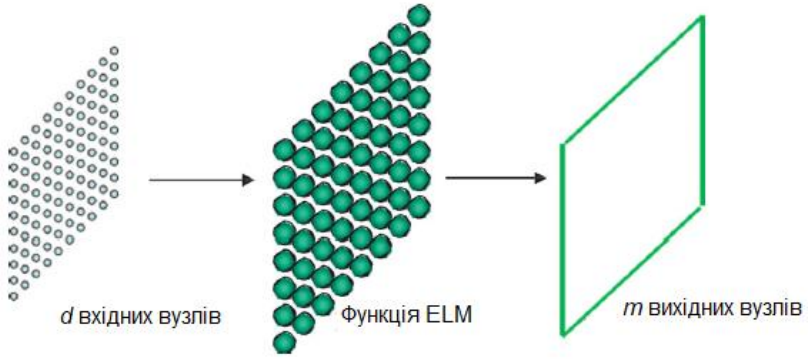

Рисунок 3.5 Елемент ELM працює як вхід для інших моделей навчання

1. На відміну від ELM та глибокого навчання, які вивчають представлення функцій на кожному рівні, SVM та LS-SVM не враховують представлення функцій та функціонуючі ролі кожного внутрішнього прихованого рівня (рис. 3.6).

2. SVM та LS-SVM також можна розглядати як мережі з одним прихованим рівнем з функцією виводу прихованого рівня $\phi(x)$. У цьому випадку і ELM, і SVM / LS-SVM мають окремі приховані рівні. Однак ELM має явне відображення прихованого рівня $h(x)$ (зручно для представлення

функцій), а SVM / LS-SVM має невідоме відображення прихованого рівня $\phi(x)$ (незручне для представлення функцій).

3. ELM працює для вивчення функцій, регресії кластеризації та класифікації з умовою оптимізації регресії хребта, в той час як SVM / LS-SVM працює в основному для двійкової класифікації з умовою оптимізації максимального запасу. Для SVM / LS-SVM складно представити функції через невідоме відображення $\phi(x)$ (в таблиці 3.1 наведено детальне порівняння ELM та SVM / LS-SVM, [35] для детального аналізу причин чому SVM і LS-SVM взагалі дають неоптимальні рішення).

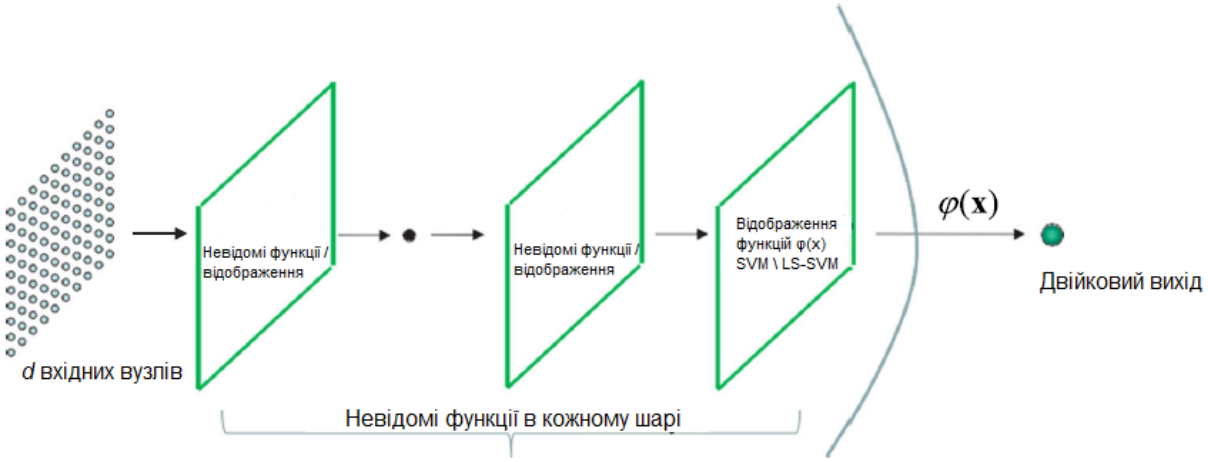

Рисунок 3.6 Взаємозв'язки та відмінності між ELM, SVM \ LS-SVM та глибоким навчанням: На відміну від ELM та глибокого навчання, (1) SVM \ LS-SVM як багатошарові мережі не підкреслює представлення функцій у прихованих шарах; та (2) SVM \ LS-SVM обробляє лише бінарні випадки безпосередньо в їх початковій формулі φ(x)

Таблиця 3.1 Порівняння співвідношення та відмінностей між ELM та SVM / LS-SVM

Властивості	ELM	SVM	LS-SVM
	На відміну від звичайних теорій навчання та загального розуміння, віра ELM: Навчання	Немає такої віри (Якщо не існує навчального рішення для мереж прямого зв'язку, потрібно лише	Немає такої віри (Якщо не існує навчального рішення для мереж прямого зв'язку, потрібно

	може бути здійснено без налаштування прихованих нейронів у широкому типі біологічних механізмів навчання та широких типів нейронних мереж	розглядати вихідні данні останнього прихованого шару: $\phi(x)$)	лише розглядати вихідні данні останнього прихованого шару: $\phi(x)$)
Функції мережевого виводу	$f_L(x) = \sum_{i=1}^{L} \beta_i G(a_i, b_i, x)$	$f(x) = \sum_{s=1}^{N_s} \alpha_s t_s \phi(x) \times \phi(x_s) + b$	$f(x) = \sum_{i=1}^{N} \alpha_i t_i \phi(x) \times \phi(x_i) + b$
Мультикласова класифікація	Прямі рішення	Непрямі рішення на основі двійкового (t_i=0 або 1) випадку	
Явні відображення функції	Так (Широкі типи явних відображень функцій h(x). Також можуть використовуватися ядра.)	Ні (Невідоме відображення $\phi(x)$, лише ядро.)	Ні (Невідоме відображення $\phi(x)$, лише ядро.)
Типи прихованих вузлів (математична модель)	Широкі типи (сигмоїд, ядро, ряд Фур'є тощо)	Ядра	Ядра

Типи прихованих вузлів (біологічні нейрони)	Так	Ні	Ні
Домен	Як реальні, так і складні домени	Реальні домени (Складно обробляти складні домени напряму)	Реальні домени (Складно обробляти складні домени напряму)
SLFN	"Узагальнені" широкі типи SLFN	Ні	Ні
Порівневе відображення функцій	Так	Ні (Представлення функцій у різних рівнях ігнорується)	Ні (Представлення функцій у різних рівнях ігнорується)
Підключення	Для повністю підключеної і для випадково (частково) підключеної мережі	Немає уваги на мережевих з'єднаннях	Немає уваги на мережевих з'єднаннях
Гіперплощинні обмеження в подвійній задачі	Ні (У нього немає таких обмежень гіперплощини через відсутність зміщення b у вихідних вузлах.)	Так (У нього є такі обмеження гіперплощини через зміщення b у вихідних вузлах.)	Так (Вона також надає модель без b, але все ще припускає бінарний клас.)
Можливість	Теоретично	Немає	Немає

універсальної апроксимації і класифікації	доведено для широких типів нелінійних часткових вузлів/ нейронів	теоретичних доказів	теоретичних доказів

Типи прихованого нейрона

На відміну від Шмідта та Пао, в якому кожен вузол є сигмоїдною або RBF функцією, ELM справедливий для широких типів нейронних вузлів та не нейронних вузлів. ELM ефективний і для вивчення ядер [35].

Реальний домен

Оскільки ELM має універсальну апроксимативну здатність для широкого типу нелінійних частково-неперервних функцій *G(a,b,x)* це не потребує зміщення на вихідному рівні. Деякі часто використовувані функції активації, що містяться в теоріях ELM [36]:

1. Сигмоїдна функція

$$G(a,b,x) = \frac{1}{1+\exp(-(a\times x+b))} \quad (3.4)$$

2. Функція Фур'є:

$$G(a,b,x) = \sin(a \times x + b) \quad (3.5)$$

3. Функція жорсткого обмеження:

$$G(a,b,x) = \begin{cases} 1, & if\ a \times x - b \geq 0 \\ 0, & \text{інакше} \end{cases} \quad (3.6)$$

4. Гаусова функція:

$$G(a,b,x) = \exp(-b\|x-a\|^2) \quad (3.7)$$

5. Функція мультиквадриків:

$$G(a,b,x) = (\|x-a\|^2 + b^2)^{1/2} \quad (3.8)$$

6. Вейвлет:

$$G(a,b,x) = \|a\|^{-1/2}\Psi(\frac{x-a}{b}) \quad (3.9)$$

де Ψ - функція вейвлет-одиночної матері.

Через застосовність універсальної апроксимації та можливості класифікації для загальних нелінійних частково-неперервних функцій

активації в ELM можуть використовуватися комбінації різних типів прихованих нейронів [39].

Складний домен

За даними Лі, випадкові приховані вузли, що використовуються в ELM, можуть бути повністю складними прихованими вузлами, запропонованими Кімом та Адалі [40], і отриманий ELM у складному домені також має можливість універсальної апроксимації. Складні приховані вузли ELM включають, але не обмежуються ними:

1. Кругові функції:

$$\tan(z) = \frac{e^{iz}-e^{-iz}}{i(e^{iz}+e^{-iz})} \quad (3.10)$$

$$\sin(z) = \frac{e^{iz}-e^{-iz}}{2i} \quad (3.11)$$

2. Зворотні кругові функції:

$$\arctan(z) = \int_0^z \frac{dt}{1+t^2} \quad (3.12)$$

$$\arccos(z) = \int_0^z \frac{dt}{(1-t^2)^{1/2}} \quad (3.13)$$

3. Гіперболічні функції:

$$\tanh(z) = \frac{e^{z}-e^{-z}}{e^{z}+e^{-z}} \quad (3.14)$$

$$\sinh(z) = \frac{e^{z}-e^{-z}}{2} \quad (3.15)$$

4. Зворотні гіперболічні функції:

$$\operatorname{arctanh}(z) = \int_0^z \frac{dt}{1-t^2} \quad (3.16)$$

$$\operatorname{arcsinh}(z) = \int_0^z \frac{dt}{(1+t^2)^{1/2}} \quad (3.17)$$

3.4 Регуляризація мережі та узагальнення продуктивності

Подібно до більшості звичайних алгоритмів навчання, запропонованих у 1980-1990-х роках, Шмідт та Пао зосередили увагу на мінімізації лише помилок у навчанні. Вони не є мережами регуляризації.

Однак, натхненні теоріями ефективності узагальнення нейронних мереж, запропонованими у 1998 р., опублікованими після Шмідта та Пао, теорія ELM має на меті досягти найменшої похибки навчання та найменшої норми вихідних вагів [40] (у цьому сенсі, загалом кажучи, ELM є різновидом

регуляризаційних нейронних мереж, але з не налаштованим відображенням прихованого рівня (утворений або випадковими прихованими вузлами, ядрами або іншими реалізаціями)):

Мінімізувати:

$$\|\beta\|_p^{\sigma_1} + C\|H\beta - T\|_q^{\sigma_2}$$

(3.18)

де $\sigma_1 > 0, \sigma_2 > 0,\ p, q = 0, \frac{1}{2}, 1, 2, \ldots, +\infty$.

Різні комбінації $\|\beta\|_p^{\sigma_1}$ і $\|H\beta - T\|_q^{\sigma_2}$ можуть бути використані і призводити до різних алгоритмів навчання для навчання функцій та кластеризації [40]. H – вихідна матриця прихованого рівня ELM (рандомізована матриця):

$$H = \begin{bmatrix} h(x_1) \\ \vdots \\ h(x_N) \end{bmatrix} = \begin{bmatrix} G(a_1, b_1, x_1) & \cdots & G(a_L, b_L, x_1) \\ \vdots & \vdots & \vdots \\ G(a_1, b_1, x_N) & \ldots & G(a_L, b_L, x_N) \end{bmatrix}$$

(3.19)

і T - цільова матриця навчальних даних:

$$T = \begin{bmatrix} t_1^T \\ \vdots \\ t_N^T \end{bmatrix} = \begin{bmatrix} t_{11} & \cdots & t_{1m} \\ \vdots & \vdots & \vdots \\ t_{N1} & \ldots & t_{Nm} \end{bmatrix}$$

(3.20)

Можна лінійно застосувати багато рішень ELM (але не всі) до конкретної сигмоїдної мережі з b та мережі, що має прямий зв'язок від вхідного рівня до вихідної мережі (включаючи, але не обмежуючись цим, QuickNet [39] та RVFL; будуть досягнуті субоптимальні рішення порівняно з оригінальними ELM. Отримані алгоритми навчання можуть бути віднесені відповідно до ELM+b та ELM+αx.

Для RVFL вихідна матриця прихованого рівня має вигляд:

$$H_{RVFL} = \begin{bmatrix} g_{sig,RBF(a_1,b_1,x_1)} & \cdots & g_{sig,RBF(a_L,b_L,x_1)} & x_1 \\ \vdots & \vdots & \vdots & \vdots \\ g_{sig,RBF(a_1,b_1,x_N)} & \cdots & g_{sig,RBF(a_L,b_L,x_N)} & x_N \end{bmatrix}$$

$$= \left[H_{\text{ELMдлясигмоїдноїабоRBFоснови}} \quad X_{N\times d}\right]$$

(3.21)

де $H_{\text{ELMдлясигмоїдноїабоRBFоснови}}$ - це дві специфічні вихідні матриці прихованого рівня ELM (19) із сигмоїдною або RBF-основою, а $X_{N\times d}$ - матриця $N\times d$ d з i-м входом x_i в якості i-го рядка. Якщо зміщення вихідного нейрона розглядатиметься як нейрон зміщення у прихованому рівні, як це зроблено в більшості звичайних нейронних мереж, вихідна матриця прихованого рівня для Шмідта буде

$$H_{\text{Шмідт}} = \begin{bmatrix} g_{sig(a_1\times x_1+b_1)} & \cdots & g_{sig(a_L\times x_1+b_L)} & 1 \dots 1 \\ \vdots & \vdots & \vdots & \vdots \\ g_{sig(a_1\times x_N+b_1)} & \cdots & g_{sig(a_L\times x_N+b_L)} & 1 \dots 1 \end{bmatrix}$$

$$= \left[H_{\text{HELMдлясигмоїдноїоснови}} \quad 1_{N\times m}\right]$$

(3.22)

де $H_{\text{ELMдлясигмоїдноїоснови}}$ - це специфічна вихідна матриця прихованого рівня ELM (19) з сигмоїдною основою, а $1_{N\times m}$ - матриця $N\times m$ з постійним елементом 1. Хоча зміщення b у Шмідта здається простим параметром, однак відомо, що з точки зору математичного та машинного навчання параметр може призвести до значних відмінностей. Його роль привернула увагу дослідників [36]. Насправді, одна з основних причин, чому протягом останніх двох десятиліть було важко застосувати SVM та LS-SVM у багатокласних програмах, головним чином, пов'язана зі зміщенням вихідного вузла b. Без зміщення вихідного вузла b, рішення SVM та LS-SVM стали б набагато простішими.

Висновки до розділу

Проаналізовано концепцію алгоритму машини екстремального навчання. Було виділено основні положення алгоритму та показано його основну задачу, якою є подолання бар'єру між звичайними методами штучного навчання та механізмом біологічного навчання. "Машина екстремального навчання" (ELM) "являє собою набір методів машинного навчання, в яких приховані нейрони не потрібно налаштовувати з урахуванням теорії узагальнення нейронних мереж, теорії управління, теорії матриць та теорії лінійних систем". ELM направлена на реалізацію п'яти основних операцій: стиснення, вивчення функцій, кластеризація, регресія та класифікація.

Теорії ELM вперше показали, що всі приховані вузли / нейрони можуть бути не тільки незалежними від навчальних зразків, але й незалежними один від одного в широких типах нейронних мереж і математичних серій / розширень, а також у механізмі біологічного навчання. Кожен прихований вузол в ELM може бути підмережею інших вузлів, в яких функціональне навчання може бути реалізовано ефективно.

Було узагальнено продуктивність кожного з алгоритмів. У результаті аналізу було виділено можливість універсальної апроксимації і класифікації машини екстремального навчання.

Досліджено зв'язок серед алгоритмів екстремального машинного навчання, глибокого навчання та SVM/LS-SVM. Було виділено основні відмінності:

На відміну від ELM та глибокого навчання, SVM та LS-SVM не враховують представлення функцій та функціонуючі ролі кожного внутрішнього прихованого рівня. SVM та LS-SVM також можна розглядати як мережі з одним прихованим рівнем з функцією виводу прихованого рівня $\phi(x)$. Однак ELM має явне відображення прихованого рівня $h(x)$

ELM працює для вивчення функцій, регресії кластеризації та класифікації з умовою оптимізації регресії хребта, в той час як SVM / LS-SVM працює в основному для двійкової класифікації з умовою оптимізації максимального запасу.

Було узагальнено продуктивність кожного з алгоритмів. У результаті аналізу було виділено можливість універсальної апроксимації і класифікації машини екстремального навчання.

РОЗДІЛ 4
ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ МЕРЕЖІ З ВИКОРИСТАННЯМ ПРАВИЛ І АЛГОРИТМУ МАШИНИ ЕКСТРЕМАЛЬНОГО НАВЧАННЯ

Бездротова сенсорна мережа складається з бюджетних сенсорних вузлів низької потужності. Сенсорні вузли контролюють події та передають дані на базову станцію [25]. Дані, зібрані з датчиків, передаються на базову станцію періодично, постійно або на основі подій.

Оскільки датчики мають обмежені ресурси, такі як простір для зберігання даних, обчислювальну потужність та енергію, зловмисники можуть легко вплинути на них [26]. Зловмисники фізично компрометують сенсорні вузли, скидають або змінюють пакети даних. Багато систем запобігання вторгненням (IPS) розроблено шляхом вивчення особливостей нападу [27], але IPS не може протистояти всім атакам. Отже, система виявлення вторгнень (IDS) використовується як другий рівень захисту для фільтрації аномальних пакетів у мережі.

У запропонованій гібридній системі IDS алгоритм правил і машини екстремального навчання (RELM) для бездротової сенсорної мережі використовується для виявлення міжрівневих атак та зменшення споживання енергії. IDS на основі правил реалізується на кожному сенсорному вузлі для виявлення міжрівневих атак. Міжрівневі правила фільтрують атаки фізичного рівня, канального рівня, мережевого рівня та прикладного рівня. Після фільтрації атак, звичайні пакети передаються на базову станцію. Таким чином, загальна кількість пакетів, що передаються на базову станцію, зменшується за рахунок впровадження IDS на кожному сенсорному вузлі в мережі. Зменшення передачі пакетів призведе до зниження енергоспоживання мережі.

Відфільтровані звичайні пакети від сенсорних вузлів далі передаються до IDS базової станції, де реалізовано ELM. Якщо атаки будуть виявлені

знову, адміністратору видається попередження для вжиття необхідних заходів, в іншому випадку дані приймаються.

4.1 Запропонована модель системи

Запропонована модель системи показана на рис. 4.1. Сенсорні вузли розгорнуті майже на всіх типах програм моніторингу. В даний час моніторинг в промисловості використовує безліч датчиків для спостереження за навколишнім середовищем та для моніторингу промислового обладнання.

Відправлення помилкової інформації адміністратору створює складну проблему в цих середовищах. Отже, в цій роботі пропонується гібридна система RELM, яка є гібридом моделі виявлення неправильного використання та аномалій.

В RELM реалізовані дві фази виявлення вторгнень. У фазі 1 кожний сенсорний вузол виявляє аномальні пакети на основі правил виявлення неправомірного втручання. Зокрема, міжрівневе виявлення вторгнень на основі правил використовується для фільтрації атак фізичного, канального, мережевого та прикладного рівнів. Цей початковий механізм фільтрації зменшує об’єм передачі пакетів до базової станції, що зменшує споживання енергії сенсорної мережі.

Аналогічно, правила виявлення неправомірних вторгнень визначають шаблони атак за відомими вразливими місцями системи. Правила оформлені експертами і такі системи виявлення неправомірних вторгнень можуть не відфільтровувати атаки, які відрізняються від визначених моделей атак. Отже, на базовій станції реалізований IDS на основі аномалій.

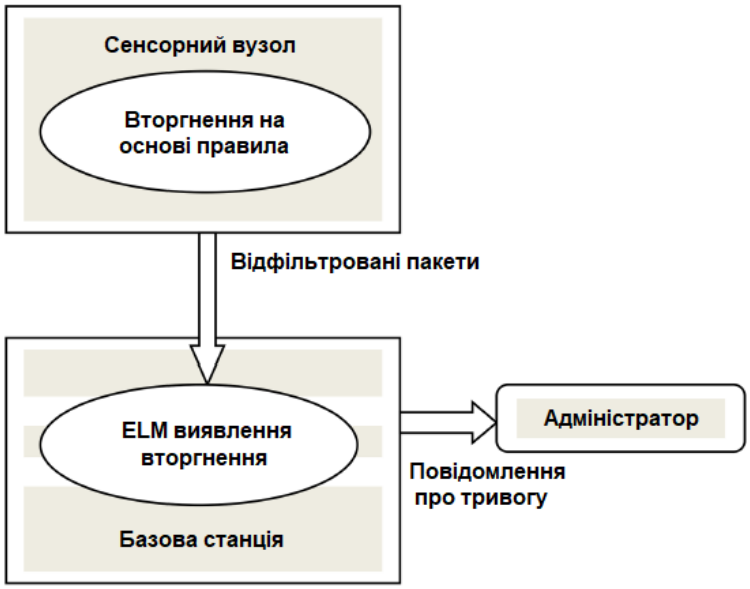

Рисунок 4.1 Модель системи

На другому етапі, гібридна система реалізується за допомогою алгоритму ELM. Ця IDS фільтрує дані, які відхиляються від нормальної поведінки. Пакети, відфільтровані на базовій станції, розглядаються як аномальні, і адміністратору передається попереджувальне повідомлення.

Впровадження методів машинного навчання споживає більше обчислювальної потужності, ніж IDS на основі правил. Оскільки базова станція є більш потужною, ніж сенсорні вузли, методика машини екстремального навчання реалізована на IDS базової станції, а самі правилах реалізовані на IDS сенсорних вузлах [41].

4.2 Міжрівневі атаки та правила їх виявлення

Більшість IDS було запропоновано для виявлення атак одного рівня бездротової сенсорної мережі [42]. Цей тип підходу називають шаруватим, і його обмеження наведені нижче:

1. забезпечує безпеку лише для одного рівня, для фізичного, канального або мережевого рівня;
2. захист одного рівня від атак та залишення всіх інших рівнів без захисту призводить до слабшого рішення безпеки;

Таким чином, система RELM зосереджується на виявленні міжрівневих атак. Експерти визначили багато правил для виявлення атак фізичного, канального, мережевого та прикладного рівнів. Система RELM аналізує правила, які використовуються в існуючих IDS, і вибирає найкращий серед них, як показано в останній колонці таблиці 4.1.

В таблиці 4.1 перераховані атаки різних рівнів, вплив на сенсорні мережі та правила виявлення. Усі правила, згадані в таблиці 4.1, використовуються в сенсорних вузлах для фільтрації аномальних пакетів. З аналізу літератури [42] видно, що не було внесено достатнього внеску у виявленні атаки помилкового ідентифікатора, атаки помилкової маршрутизації і атаки вибіркового пересилання повідомлень. Таким чином, система RELM визначає нові правила виявлення атаки помилкового ідентифікатора канального рівня, атаки помилкової маршрутизації мережевого рівня та атаки вибіркового пересилання повідомлень прикладного рівня. Ефекти та правила виявлення цих атак показані в таблиці 4.1.

Таблиця 4.1 Міжрівневі атаки та правила їх виявлення

Рівень атаки	**Назва атаки**	**Вплив на сенсорні мережі**	**Правила виявлення**
Фізичний рівень	атака заклинювання (jamming) - канал блокується неперервною або випадковою передачею радіо сигналів за допомогою пристроя із	відкидування пакетів, збільшення затримки і падіння пропускної здатності	відхилення у швидкості надходження пакетів, відхилення у рівні прийнятого сигналу (RSS)

	завадами		
	атака відмови вузла (node failure attack) – вузол виходить з ладу або через відмову акумулятора, або через екологічні причини	передача даних припиняється або вводиться затримка	правило інтервалу час затримки проходження сигналу туди і назад
Канальний рівень	атака маніпуляції трафіком - стримує дані або надсилає безглузді дані	DoS-атака, спотворення агрегації даних	відхилення швидкості прийому пакетів
	атака хибного ідентифікатора - незареєстрований вузол додається у мережу	помилкове введення даних або передача даних припиняється	базова станція порівнює із зареєстрованими ідентифікаторами під час отримання даних
	Sybil атака - вводить дублікати ідентичності в мережу	дублювання вузлів	ідентичність вузла з різними значеннями RSS, правило радіопередачі
Мережевий рівень	помилкова атака даних - фактичні значення даних у пакеті будуть змінені	значення даних змінюються	правило цілісності
	атака скидування пакетів -	вибіркове або повне	скидування пакетів

	скидування пакетів даних	скидування пакетів даних	
	помилкова атака маршрутизації - помилковий шлях маршрутизації	помилкова атака даних або затримка	збільшення затримки та зміни в RSS
	hello flood атака - атакуючий діє як сусідній вузол	затоплення hello пакетів, фальшива атака даних, скидування пакетів	додавання нового ідентифікатора вузла
Прикладний рівень	вибіркова переадресація повідомлень	зміни значення агрегації даних	правило цілісності

Таблиця 4.2 Набір даних NSL-KDD

Загальна кількість записів	**Кількість атак**	**Кількість нормальних даних**
125,973 навчальних записів	58,630	67,343
22,544 тестових записів	12,834	9710

Таблиця 4.3 Тестовий набір даних

Тестові записи	**Загальна кількість тестових записів**	**Кількість атак**	**Кількість нормальних даних**

1	22,544	12,834	9710
2	11,272	6430	4842
3	7515	4345	3170

Таблиця 4.4 Виконання методів класифікації на тестовому записі 1

	BPN	**SVM**	**ELM**
Істино позитивний (TP)	9040	9320	9600
Хибно негативний (FN)	670	390	110
Хибно позитивний (FP)	623	354	90
Істино негативний (TN)	12,211	12,480	12,744
Істина позитивна норма (TPR)	93.09	95.98	98.86
Істина негативна норма (TNR)	95.14	97.24	99.29
Точність, %	93.55	96.34	99.07
Акуратність, %	94.26	96.7	99.11

4.3 Використання алгоритму ELM для виявлення аномалій

Виявлення аномалій вторгнень реалізується на базовій станції за допомогою алгоритму машини екстремального навчання. Метод виявлення аномалії визначає всю нормальну поведінку пакетів. Його реалізація на основі алгоритмів машини навчання споживає більше енергії, що не є можливим на вузлах датчиків. Отже, алгоритми машинного навчання реалізовано на базовій станції.

Алгоритми машинного навчання поділяються на два типи контрольованого та непідконтрольного навчання. Інакше керовані алгоритми навчання відомі як класифікація. У контрольованих моделях навчання є

навчальні дані для вивчення співвідношення між входом і виходом, тоді як алгоритм непідконтрольного навчання за навчанням не має жодних навчальних даних, алгоритм робить прогнози щодо організації даних. Інакше він відомий як кластеризація. Система RELM використовує алгоритм навчання, що контролюється ELM, оскільки вона має класифікувати нормальні та аномальні пакети.

ELM - це нейромережа, що рухається вперед, з одно- або декількома рівнями прихованих вузлів. Вхідні ваги та зміщення прихованих вузлів можуть бути визначені випадковим чином, а ваги, що з'єднують вихідний шар та прихований шар, можна визначати аналітично [43]. Час навчання алгоритму ELM набагато швидше, ніж у нейронній мережі зворотного поширення (BPN), тому що вихідні ваги прихованих вузлів вивчаються за один крок [44]. Нижче показаний алгоритм ELM прихованого шару.

Вихідна функція і-го прихованого вузла задається як:

$$h_i(x) = G(a_i, b_i, x)$$

(4.1)

де a_i і b_i - параметри *i*-го прихованого вузла.

Вихідною функцією ELM є:

$$f_L(x) = \sum_{i=1}^{L} \beta_i h_i(x)$$

(4.2)

де L - кількість прихованих вузлів, а β_i - вихідна вага *i*-го прихованого вузла.

Приховане відображення рівня шару є:

$$h(x) = [G(h_i(x), \dots, h_L(x))]$$

(4.3)

Аналогічно, виведена матриця H прихованого шару задається як:

$$H = \begin{bmatrix} h(x_1) \\ \vdots \\ h(x_N) \end{bmatrix} = \begin{bmatrix} G(a_1, b_1, x_1) & \cdots & G(a_L, b_L, x_1) \\ \vdots & \vdots & \vdots \\ G(a_1, b_1, x_N) & \dots & G(a_L, b_L, x_N) \end{bmatrix}$$

(4.4)

, де N - навчальні зразки

Матриця цільових даних навчальних даних задається як:

$$T = \begin{bmatrix} t_1 \\ \vdots \\ t_N \end{bmatrix}$$

(4.5)

Простий алгоритм ELM використовує форму:

$$\hat{Y} = W_2\sigma(W_1 x)$$

(4.6)

, де W_1 - матриця вхідних ваг прихованого шару, W_2 - матриця вихідних ваг прихованого шару, а σ - функція активації. Алгоритм працює наступним чином:

(i) випадкові значення призначаються вхідним вагам прихованого шару W_1;

(ii) обчислити W_2 за найменшими квадратами, що підходять до матриці відповіді.

змінні Y з використанням псевдоінверсії +.

Дизайн-матриця X задається як:

$$W_2 = \sigma(W_1 X)^+ Y$$

(4.7)

4.4 Результати експериментів

У системі RELM алгоритм ELM порівнюється з двома іншими стандартними алгоритмами класифікації, а саме BPN та SVM на наборі даних NSL-KDD [45]. Набір даних NSL-KDD доступний в університеті Нью-Брансвіку, Канада [45]. Набір даних NSL-KDD складається з 125 973 записів про навчання та 22 554 записів про тестування.

У таблиці 4.2 показано кількість атак та нормальних даних у записах тренувань та тестувань набору даних NSL-KDD. Набір навчальних даних і тестування містить 41 атрибут, який визначає особливості мережі, а 42-й атрибут має п'ять міток класу із зазначенням нормальних або чотирьох мережевих атак. Чотири мережеві атаки - це атака відмови в обслуговуванні

(DoS), віддалена локальна атака, коренева атака на користувача та атака зондування.

Реалізація методів класифікації виконується на комп'ютерній системі процесора Intel Core i5 2,66 ГГц з процесором 4 Гб оперативної пам’яті за допомогою MATLab. Методи класифікації реалізуються на різних тестових наборах даних. Деталі різних тестових записів наведені в таблиці 4.3.

Продуктивність BPN, SVM та ELM оцінюється за істиною позитивною швидкістю (TPR), істиною негативною швидкістю (TNR), точністю та акуратністю, використовуючи формулу, наведену нижче:

$$TPR\ (\text{чутливість}) = \frac{TP}{TP+FN} \quad (4.8)$$

$$TNR\ (\text{чутливість}) = \frac{TN}{TN+FP} \quad (4.9)$$

$$\text{Точність} = \frac{TP}{TP+FP} \quad (4.10)$$

$$\text{Акуратність} = \frac{TP+TN}{TP+TN+FP+FN} \quad (4.11)$$

У таблицях 4.4–4.6 наведено порівняння ефективності BPN, SVM та ELM у різних тестових записах.

Таблиця 4.5 Виконання методів класифікації на тестовому записі 2

	BPN	SVM	ELM
TP	4500	4720	4788
FN	342	122	54
FP	428	130	78
TN	6002	6300	6352
TPR	92.93	97.48	98.88
TNR	93.34	97.97	98.78
Точність, %	91.31	97.32	98.39

Акуратність, %	93.16	97.76	98.82

Таблиця 4.6 Виконання методів класифікації на тестовому записі 3

	BPN	SVM	ELM
TP	3000	3110	3140
FN	170	60	30
FP	445	340	238
TN	3900	4005	4107
TPR	94.63	98.10	99.05
TNR	89.75	92.17	94.52
Точність, %	87.08	90.14	92.95
Акуратність, %	91.81	94.67	96.43

Таблиця 4.7 Десятикратна перехресна перевірка

	Неправильно класифіковані	Правильно класифікований	Точність
BPN	888.3	13,963.4	94.01887
SVM	577.2	14,274.5	96.11358
ELM	193.7	14,658	98.69577

Таблиця 4.8 Частота виявлення атак, використовуючи міжрівневі правила для набору даних у реальному часі

Атаки	1000		2300		4600		5600	
	Кількість атак	DR, %	Кількість атак	DR, %	Кількість атак	DR, %	Кількість атак	DR, %
атака заклинювання	14	72	21	71	28	70	30	70
атака відмови вузла	20	85	21	81	29	76	31	68

атака маніпуляції трафіком	20	90	27	89	31	87	35	80
атака хибного ідентифікатора	13	85	20	90	27	74	33	60
Sybil атака	12	92	21	86	27	85	31	81
Атака реплікації пакетів	19	79	25	88	30	87	36	84
Атака зміненого пакета	16	94	20	75	25	80	30	70
атака скидування пакетів	14	93	19	76	26	70	33	70
Атака помилкової маршрутизації	18	72	21	76	27	78	32	54
Hello flood атака	16	87	20	90	26	81	30	77
Вибіркова переадресація повідомлень	17	94	24	84	29	80	31	71

BPN, SVM та ELM тестуються за допомогою трьох тестових записів. Частота виявлення (DR) ELM висока у порівнянні з BPN та SVM у всіх трьох тестових випадках. Оскільки в ELM, вихідні ваги прихованих вузлів вивчаються за один крок, лише вхідні ваги прихованих вузлів потрібно оновлювати до досягнення цільового значення з прийнятною швидкістю. Середній показник швидкості виявлення, досягнутий за допомогою ELM серед усіх тестових випадків, становить 97,53%.

У таблиці 4.7 наведені результати десятикратної перехресної перевірки. Перехресне оцінювання використовується для оцінки здатності до

узагальнення трьох методів класифікатора, таких як BPN, SVM та ELM. У десятикратній перехресній валідації весь набір даних поділяється на десять підмножин. При кожному разі, дев'ять підмножин зберігаються для навчання, а одна підмножина використовується для тестування.

Процес перехресної перевірки повторюється десять разів, зберігаючи кожну підмножину як тестові дані без повторення, і точність обчислюється для кожного разу. Нарешті, обчислюється середнє значення точності для всіх десяти раз.

Експериментальні результати в реальному часі

Для кращого розуміння наслідків запропонованих методів та щоб переглянути характер даних із датчиків, було проведено дослідження на сенсорних вузлах, що використовуються в системі спостереження. Було використано два найпопулярніші сенсорні вузли - це пасивний інфрачервоний датчик та ультразвуковий датчик [46]. Ці два вузли підключені до мікроконтролера і передають дані руху об'єктів та відстань предметів до цільового місця.

Набір даних реального часу створюється за допомогою даних, сформованих з цих двох датчиків. Дані зберігаються на базовій станції та перевіряються відповідно до правил міжшарового рівня, визначених у таблиці 4.1. Мова Java використовується для створення інтерфейсу та для виявлення атак зібраного набору даних у реальному часі. Кількість нападів та DR атаки для 1000, 2300, 4600 та 5600 наборів даних наведено в Таблиці 4.8.

Тестовий запис 5600 береться як зразок для аналізу. Загальна кількість атак та нормальних даних у наборі даних у режимі реального часу 5600 - 352 та 5248. З 352 атак 251 атаку виявлено за допомогою правил міжшарового рівня. Таким чином, запис тесту скорочується до 5349. Оскільки 71% атак виявляються за допомогою правил на рівні шарів, споживання енергії або передача пакетів на базову станцію зменшується. Деталі запису випробувань у режимі реального часу наведені в таблиці 4.9.

Таблиця 4.9 Тестові записи в реальному часі

Тестовий запис	Тестовий запис в реальному часі	Загальна кількість записів тестування	Кількість атак	Кількість нормальних даних
4	без застосування міжрівневих правил	5600	352	5248
5	після застосування міжрівневих правил	5349	101	5248

Таблиця 4.10 Продуктивність ELM на тестових записах 4 і 5

ELM	Без застосування міжрівневих правил	Після застосування міжрівневих правил
TP	5190	5190
FN	58	58
FP	28	2
TN	324	99
TPR	98.89	98.89
TNR	92.04	98.01
Точність, %	99.46	99.96
Акуратність, %	98.46	98.87

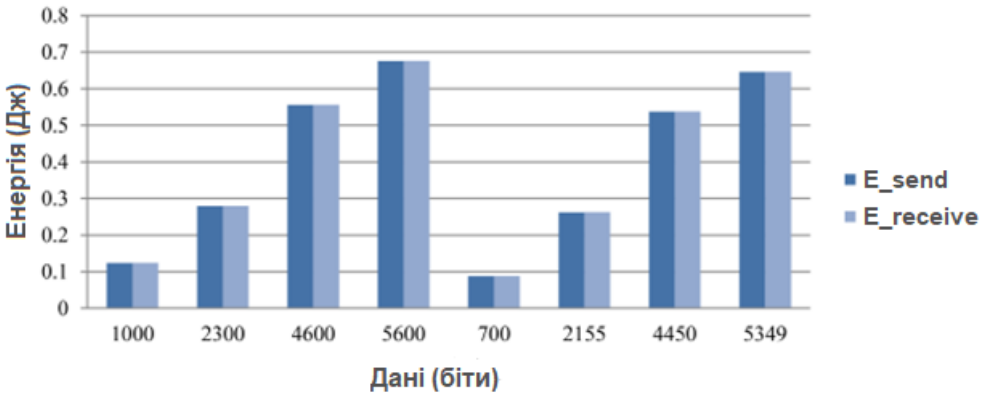

Рис.4.2 Споживання енергії сенсорного вузла

Результати моделювання показують, що продуктивність ELM краща, ніж BPN та SVM. ELM реалізований на тестових записах 4 та 5, а його

ефективність показана в таблиці 4.10. Загальна DR атаки становить 98,01% за допомогою правил міжшарового рівня та ELM, а DR атаки ELM без застосування правил міжшарового рівня становить 92,04%.

Витрата енергії сенсорного вузла залежить від енергії, необхідної для відправки, обробки та отримання пакетів у БСМ. Якщо на 10% збільшиться кількість інструкцій для виконання у вузлі, це призведе до збільшення на 2% споживання енергії вузла [47]. У запропонованому RELM передача пакетів знижується шляхом виявлення атак. Врешті-решт, споживання енергії всіх інших приймальних вузлів або вузлів наступної ієрархії рівня зменшиться. Енергія, необхідна для відправки та отримання пакетів, обчислюється за формулою, наведеною нижче [48]:

$$E_{send} = m_{send} \times n + b_{sendmJ} \quad (4.12)$$

$$E_{receive} = m_{receive} \times n + b_{receivemJ} \quad (4.13)$$

У формулі m_{send} і $m_{receive}$ - енергія, необхідна для надсилання та прийому 1 байта, n - розмір пакету, а b_{send} і $b_{receive}$ - накладні витрати каналу. мДж означає міліюле. Значення m_{send} і $m_{receive}$ в Tmote Sky становить 0,12 мДж, а значення b_{send} і $b_{receive}$ відповідно 3,54 та 4,03 [48]. При цьому енергія, необхідна для відправки пакетів, береться на аналіз.

Енергія, необхідна для відправки 1000, 2300, 4600, 5600 пакетів, вища, ніж відправлення пакетів після міжшарової фільтрації IDS. Атаки зменшуються на 71% після міжшарової фільтрації IDS у вузлах датчика. Отже, загальна кількість пакетів, що передаються, зменшується до 875, 2155, 4450 і 5349 відповідно. Енергія, необхідна для відправки та прийому пакетів у сенсорному вузлі при використанні лише міжшарової фільтрації IDS у вузлах датчика, показана на рис. 4.2.

При використанні ELM атаки зменшуються на 98%, а кількість пакетів, що передаються, зменшуються відповідно до 822, 2066, 4298, 5250. У результаті в системі передається у середньому на 9% менше пакетів чим без

використання RELM системи. Енергія, необхідна для відправки та прийому пакетів у сенсорному вузлі при використанні міжшарової фільтрації IDS у вузлах датчика та ELM на базовій станції, показана на рис. 4.2.

Висновки до розділу

У запропонованій гібридній системі IDS алгоритм правил і машини екстремального навчання (RELM) для бездротової сенсорної мережі використовується для виявлення міжрівневих атак та зменшення споживання енергії. В RELM реалізовані дві фази виявлення вторгнень. У фазі 1 кожний сенсорний вузол виявляє аномальні пакети на основі правил виявлення неправомірного втручання. На другому етапі, гібридна система реалізується за допомогою алгоритму ELM. Ця IDS фільтрує дані, які відхиляються від нормальної поведінки. Пакети, відфільтровані на базовій станції, розглядаються як аномальні, і адміністратору передається попереджувальне повідомлення. Система RELM зосереджується на виявленні міжрівневих атак. Вона аналізує правила, які використовуються в існуючих IDS, і вибирає найкращий серед них.

У системі RELM алгоритм ELM порівнюється з двома іншими стандартними алгоритмами класифікації, а саме BPN та SVM на наборі даних NSL-KDD. Результати моделювання показують, що продуктивність ELM краща, ніж BPN та SVM. ELM реалізований на тестових записах. При використанні ELM атаки зменшуються на 98%,. У результаті в системі передається у середньому на 9% менше пакетів чим без використання RELM системи.

ЗАГАЛЬНІ ВИСНОВКИ ПО РОБОТІ

Зі стрімким розвитком бездротових сенсорних мереж, що повинні обробляти великі масиви даних, з'явилася необхідність оптимізації традиційної архітектури мережі для забезпечення передачі та обробки цих даних з якомога більшою ефективністю і при цьому забезпечуючи стійку роботу мережі.

Досліджено основні принципи, фундаментальні характеристики і направлення практичного застосування концепції бездротових сенсорних мереж, а також продемонстровано основні проблеми енерговикористання у цих мережах.

Визначено організацію безпеки в бездротовій сенсорній мережі. Багато механізмів виявлення та запобігання атакам безпеки розроблені для БСМ; однак більшість існуючих рішень здатні обробляти лише декілька атак безпеки. Найкраща практика для забезпечення захисту бездротових мереж полягає в тому, щоб реалізувати множину механізмів безпеки; саме тому IDS є важливим у бездротових мережах. Фільтрування атак з використанням IDS на вузлах датчиків зменшує кількість передачі пакетів до базової станції, що, в свою чергу, зменшує споживання енергії сенсорної мережі. Алгоритм машини екстремального навчання (ELM) реалізований на базовій станції для того, щоб виявляти аномальні пакети.

Проведено аналіз математичного апарату машини екстремального навчання для обробки даних у бездротовій сенсорній мережі та можливість його використання у цих мережах, для зменшення кількості анонімних пакетів передачі даних. Проведено аналіз математичного апарату машини екстремального навчання для обробки даних в бездротових сенсорних мережах та доведено можливість використання алгоритму екстремального навчання при побудові бездротової сенсорної мережі.

Модифіковано архітектуру бездротової сенсорної мережі за рахунок машини екстремального навчання для підвищення ефективності передачі та обробки даних. У запропонованій гібридній системі IDS алгоритм правил і

машини екстремального навчання (RELM) для бездротової сенсорної мережі використовується для виявлення міжрівневих атак та зменшення споживання енергії. В RELM реалізовані дві фази виявлення вторгнень. У фазі 1 кожний сенсорний вузол виявляє аномальні пакети на основі правил виявлення неправомірного втручання. На другому етапі, гібридна система реалізується за допомогою алгоритму ELM. Система RELM зосереджується на виявленні міжрівневих атак. Вона аналізує правила, які використовуються в існуючих IDS, і вибирає найкращий серед них.

У системі RELM алгоритм ELM порівнюється з двома іншими стандартними алгоритмами класифікації, а саме BPN та SVM на наборі даних NSL-KDD. Експериментальний результат показує ефективність різних методів класифікації та правил міжрівневого набору даних NSL-KDD та набору даних у режимі реального часу. Швидкість виявлення алгоритму ELM вище в порівнянні з іншими системами. Результати моделювання показують, що продуктивність ELM краща, ніж BPN та SVM. При використанні ELM атаки виявлення атак збільшується з 71% на 98%. У результаті в системі передається у середньому на 9% менше пакетів чим без використання RELM системи.

Витрата енергії сенсорного вузла залежить від енергії, необхідної для відправки, обробки та отримання пакетів у БСМ. Якщо на 10% збільшиться кількість інструкцій для виконання у вузлі, це призведе до збільшення на 2% споживання енергії вузла. У запропонованому RELM передача пакетів знижується шляхом виявлення атак. Врешті-решт, споживання енергії всіх інших приймальних вузлів або вузлів наступної ієрархії рівня зменшиться.