ДОДАТОК А

Графічний матеріал кваліфікаційної роботи

Харківський національний університет радіоелектроніки

каф. ЕОМ

Модель мультиагентної системи виявлення вторгнень

Ст.гр.СПм-23-4
Дубихвіст В.В

Керівник
доцент Ляшенко О.С.

2025

Актуальність роботи

З популярністю технології Інтернету речей (IoT) безпека мережі IoT стала важливою проблемою. Традиційні системи виявлення вторгнень мають свої обмеження при застосуванні до мережі IoT через обмеження ресурсів і складність.

Дослідження в рамках кваліфікаційної роботи зосереджено на розробці, реалізації та тестуванні системи виявлення вторгнень, яка використовує гібридну стратегію розміщення на основі мультиагентної системи, блокчейну та алгоритмів глибокого навчання.

Мета та задачі кваліфікаційної роботи

Мета кваліфікаційної роботи запропонувати модель мультиагентної системи виявлення вторгнень.

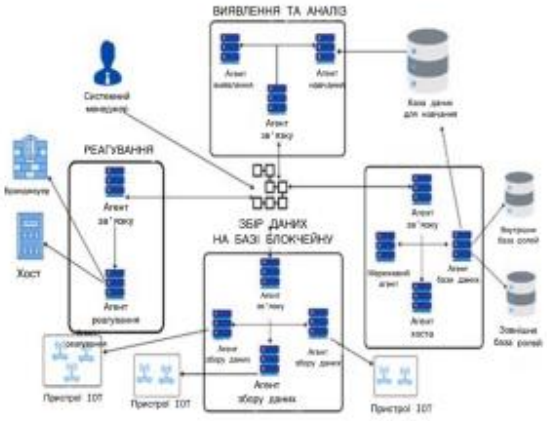
Задачі:

- Провести аналіз функціонування систем виявлення вторгнень
- Запропонувати модель мультиагентної системи виявлення вторгнень
- Розробити модулі запропонованої системи
- Провести тестування створеної системи використовуючи набір даних NSL-KDD

3

Система виявлення вторгнень

- Система виявлення вторгнень, описана на рисунку, використовує мультиагентну технологію.
- Кожен агент є відносно незалежною одиницею. Агенти поділяються на чотири різні типи модулів.
- Вони взаємодіють один з одним через комунікаційні агенти, що знаходяться в кожному модулі. Таким чином, кожен модуль може працювати відносно незалежно, що зменшує залежності між модулями.
- Вся система складається з модуля збору, модуля обробки даних, модуля виявлення та аналізу та модуля реагування.
- Система використовує мову комунікації FIPA-ACL на основі інтелектуальних фізичних агентів та агентів як мову комунікації агентів, оскільки FIPA-ACL підтримується багатьма спільнотами.



4

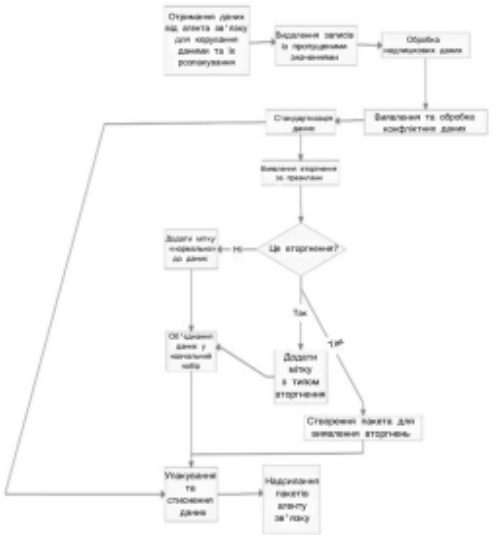
Модуль виявлення та аналізу

- Цей модуль відповідає за виявлення та аналіз шкідливого трафіку/шаблонів. Нижче описано класи Java, які ми використовували для реалізації цього модуля.
- Агент DACommunication – це комунікаційний агент модуля виявлення та аналізу. Цей процес пояснюється на рисунку.
- Після того, як модуль обробки даних надсилає повідомлення про необхідність виявлення нового пакета даних, агент DACommunication надсилає команду агенту виявлення. Коли агент виявлення завершить виявлення, агент DACommunication отримає звіт про виявлення від агента виявлення.
- Звіт про виявлення буде інкапсульовано в комунікаційний об'єкт і надіслано агенту RCommunication.
- Якщо агент DACommunication отримає комунікаційний об'єкт, який повідомляє про оновлення навчального набору, агент DACommunication надішле команду навчальному агенту.
- Після того, як навчальний агент завершить навчання моделі, звіт про навчання буде надіслано агенту DACommunication, а також агенту RCommunication.

5

Модуль обробки даних

- На рисунку відображено основну цього модуля, що є обробка даних для мережі, хоста та інших агентів.
- Агент керування мережевими даними та агент керування даними хоста обробляють дані, що надходять відповідно з мережі та хоста. Обидва агенти повинні виконувати попередню обробку даних, включаючи обробку відсутніх значень, інтеграцію даних та стандартизацію даних.
- Після етапу попередньої обробки дані будуть скановані на основі правил виявлення вторгнень, згенерованих іншими спільнотами відкритого коду IDS та/або правил системного менеджера. Крім того, попередньо оброблені дані будуть упаковані та стиснуті.
- Виявлені поведінкові процеси вторгнення та відповідні заходи обробки записуються в пакет виявлення вторгнень. Після порівняння цього з результатом агента виявлення, пакет виявлення вторгнень надсилається агенту відповіді. Позначені дані об'єднуються в пакет навчального набору, який використовується для підвищення точності агента виявлення.



Процес роботи агентів управління даними

6

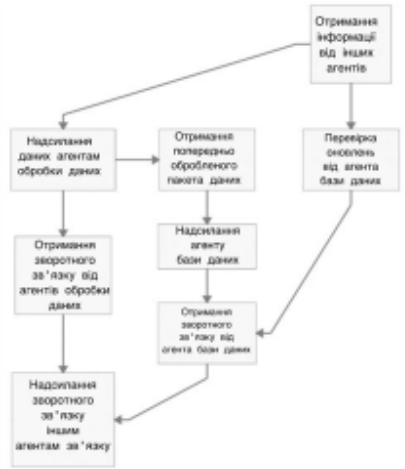
Процес агента бази даних

- Агент бази даних – єдиний агент, який може змінювати базу даних, на рисунку.
- Він може змінювати базу даних лише за наявності команди від комунікаційного агента. Після того, як агент бази даних отримає команду оновлення від комунікаційного агента, він змінює базу даних на основі даних, наданих комунікаційним агентом.
- Після того, як агент бази даних змінив базу даних, він надсилає комунікаційному агенту повідомлення зворотного зв'язку.

7

Комунікаційний агент для процесу обробки даних

- Комунікаційний агент для процесу обробки даних керує та контролює хост-агент обробки даних, мережевий агент обробки даних та агент бази даних, на рисунку.
- Він надсилає пакети даних з модуля збору агентам обробки даних, надає команди агенту обробки даних та отримує їхній зворотний зв'язок.
- Він запитує агент бази даних про регулярні перевірки оновлень, забезпечуючи актуальність системи. Цей агент також взаємодіє з іншими комунікаційними агентами та коригує свій робочий режим відповідно до стану системи.



8

Набір даних

- Набір даних NSL-KDD вирішує деякі з властивих наборів даних KDD99. Набір даних NSL-KDD широко використовується в розробці систем виявлення вторгнень. Хоча цей набір даних все ще має деякі недоліки, його можна використовувати як ефективний набір даних для порівняння різних методів виявлення вторгнень.
- Розмір навчального та тестового наборів NSL-KDD є прийнятним, а результати оцінки різних дослідників будуть узгодженими та порівнянними. Дані набору даних NSL-KDD надходять з трьох різних протоколів (протокол керування передачею (TCP), протокол користувацьких дейтаграм (UDP) та протокол керування повідомленнями Інтернету (ICMP). Набір даних NSL-KDD містить чотири класи атак (DoS, Probe, R2L, U2R) та 39 різних типів атак.
- У роботі набір даних NSL-KDD використовується як джерело даних для моделювання виявлення вторгнень.

Зразки з набору даних NSL-KDD позначені як нормальні або аномальні. 70% підмножини з назвою «Набір даних Train + 20%» використовується як навчальний набір даних, тоді як 30% набору даних «Train + 20%» використовується як набір даних для валідації. Підмножина «Набір даних Test+», що містить 1200 зразків даних, використовується як тестовий набір даних в таблицях

Типи атак Train + 20%

Основні типи атак	Типи атак
DOS	Back, Land, Neptune, Pod, smurf, teardrop
Probe	Satan, IPsweep, Nmap, portsweep
R2L	ftp_write, phf, multihop, warezmaster, guess_passwd, warezclient, imap, spy
U2R	buffer_overflow, loadmodule, rootkit

Типи атак на піднабір даних Test+

Основні типи атак	Типи атак
DOS	Back, Land, Neptune, Pod, smurf, teardrop, mailbomb, processtable, udpstorm, apache2
Probe	Satan, IPsweep, Nmap, portsweep, mscan, saint
R2L	Warezmaster, xsnoop, snmpguess, snmpgetattack, httptunnel, sendmail, named, guess_passwd
U2R	buffer_overflow, rootkit

9

Попередня обробка

- Усі необроблені дані для навчальних, валідаційних та тестових наборів даних стандартизовані за допомогою одноразового кодування та вимірювань z-оцінки, а нормалізація виконується з використанням однієї й тієї ж схеми.
- Для цього експериментального дизайну одноразове кодування використовує категоріальні змінні з усіх навчальних, валідаційних та тестових наборів даних, замість використання категоріальних змінних на основі окремих наборів даних. Одна категоріальна змінна в кожному параметрі, яку потрібно закодувати за допомогою одноразового кодування, видаляється, щоб запобігти потраплянню фіктивних змінних.
- Останнє поле «class» – це вихідна мітка. Змінні, такі як protocol_type, service та flag, містять кілька значень, тому їх потрібно перевести в числові значення за допомогою одного кодування. Щоб уникнути пастки фіктивних змінних, одне категоріальне значення protocol_type, service та flag видаляється. Поле «class» також кодується в числові значення.
- Для визначення продуктивності модуля виявлення та аналізу було порівняно продуктивність у різних ситуаціях, результати в таблицях

Точність виявлення вторгнень за різної кількості епох

Розмір пакету	Номер партії	Епоха	Точність на наборі валідації	Точність на тестовому наборі
32	300	50	98,46%	80,35%
32	300	100	98,51%	82,91%
32	300	150	98,47%	81,91%
32	300	200	98,52%	82,43%
32	300	250	98,44%	82,24%
32	300	300	98,45%	82,57%

Точність виявлення вторгнень для різних номерів партій.

Розмір пакету	Номер партії	Епоха	Точність на наборі валідації	Точність на тестовому наборі
32	50	100	97,36%	77,58%
32	100	100	97,63%	78,83%
32	150	100	98,07%	80,25%
32	200	100	98,19%	81,00%
32	250	100	98,34%	80,17%
32	300	100	98,51%	82,92%
32	350	100	98,43%	80,67%
32	400	100	98,47%	80,92%

10

Попередня обробка (2)

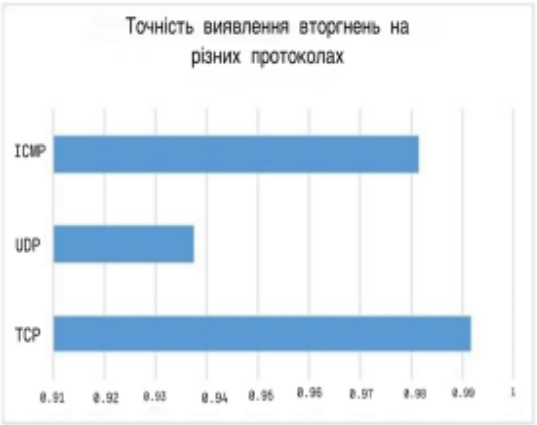
- Тестування модуля виявлення та навчання з різними розмірами партій, номерами партій та епохами показало, що модель DNN має кращу продуктивність для розміру партії 48, номера партії 300 та кількості епох 100, ніж для інших протестованих значень.
- Коефіцієнт точності з використанням валідаційного набору становить 98,27%, тоді як точність тестового набору становить 83,17%.
- Точність на тестовому наборі становить 83,53%. Повчальність на тестовому наборі становить 84,14%, а показник F1 на тестовому наборі становить 83,94%.
- Це означає, що модель DNN у цій системі має хорошу здатність відрізняти атаки від звичайного трафіку даних. Ці експерименти також показують, що вибір достатньої кількості епох може забезпечити хорошу продуктивність моделі, навіть якщо навчальний набір має менше вибірок.

Розмір партії	Номер партії	Епоха	Точність на наборі валідації	Точність на тестовому наборі
16	300	100	98,09%	81,25%
32	300	100	98,51%	82,92%
48	300	100	98,27%	83,17%
64	300	100	98,54%	80,42%
80	300	100	98,67%	79,83%

11

Точність за різними протоколами

- Якщо використовувати dst_bytes як єдиний параметр, коефіцієнт точності становить 43% для тестового набору даних, але показник F1 як для валідаційного, так і для тестового набору даних дорівнює 0%. Це означає, що всі зразки в наборах даних класифікуються як один клас, що є проблемою перенавчання. Це пояснюється тим, що деякі гіперпараметри, такі як кількість епох, є занадто високими для наборів даних з одним параметром.
- На рисунку можна побачити, що модель добре працює на наборах даних TCP та ICMP (коефіцієнт точності становить 99,1% та 98,1% відповідно). Однак коефіцієнт точності для протоколу UDP становить лише 93,7%.
- Однією з причин є те, що набір даних містить дуже мало даних з протоколами UDP. Особливості протоколу UDP є ще однією причиною. Для набору даних, який використовує клас для різних типів атак як значення, DNN має хорошу продуктивність (коефіцієнт точності становить 97%). Однак деякі типи атак, які трапляються лише у відносно невеликій кількості даних, не можуть бути добре розрізнені.



12

Висновки

У рамках кваліфікаційної роботи розглянуто та запропоновано систему виявлення вторгнень на основі багатоагентної системи, блокчейну та глибокого навчання. Детально описали режим роботи кожного компонента моделі та роботу всієї системи. Гнучкість багатоагентних систем означає, що цю нову IDS можна застосовувати в середовищах IoT різного розміру.

Усі дії, спричинені комунікаційними агентами, будуть записані на блокчейні, що робить систему захищеною від загроз, включаючи підробку інформації, розголошення інформації тощо.

Використання багатоагентного алгоритму посилення може допомогти системі постійно покращувати її продуктивність.

Експерименти з використанням набору даних NSL-KDD демонструють високу точність виявлення вторгнень на транспортному рівні середовища IoT.

Результати дослідження подані в фаховий журнал категорії Б «Вісник Вінніцкого політихнічного інстітуту» у вигляді наукової статті Ляшенко О.С., Журило О.Д, Дубихвіст В.В. Модель мультиагентної системи виявлення вторгнень (дата подачі 14.06.2025)